Guía de administración de Symantec™ IT Management Suite 7.5 con tecnología Altiris™

Guía de administración de Symantec™ IT Management Suite 7.5 con tecnología Altiris™

El software descrito en el presente manual está sujeto a un acuerdo de licencia y solamente podrá utilizarse según los términos de dicho acuerdo.

Aviso legal

Copyright © 2013 Symantec Corporation. Todos los derechos reservados.

Symantec, Altiris, el logotipo de Symantec, el logotipo de la marca de comprobación y cualquier marca registrada de Altiris o de Symantec usadas en el producto son marcas registradas o marcas comerciales registradas de Symantec Corporation o de sus afiliadas en los E.E. U.U. y otros países. Los demás nombres pueden ser marcas registradas de sus respectivos propietarios.

Este producto de Symantec puede contener software de otro fabricante que Symantec debe atribuir al otro fabricante (“Programas de otros fabricantes”). Algunos Programas de otros fabricantes están disponibles con licencias de código abierto o de software gratuito. El Acuerdo de licencia que acompaña el Software con licencia no altera ningún derecho ni obligación que pueda tener en función de esas licencias de código abierto o de software gratuito. Para obtener más información sobre los Programas de otros fabricantes, consulte el documento Aviso de otro fabricante para este producto de Symantec que puede estar disponible en http://www.symantec.com/es/mx/about/profile/policies/eulas/, el apéndice Aviso legal de otro fabricante que se puede incluir con esta Documentación o el archivo léame del aviso legal de otro fabricante que puede acompañar a este producto de Symantec.

El producto descrito en este documento se distribuye bajo las restricciones de licencia para su uso, copia, distribución e ingeniería inversa y descompilación. Ninguna parte de este documento puede ser reproducido por ningún medio o de ninguna forma sin una autorización previa por escrito de Symantec Corporation y sus titulares de licencias, si los hubiera.

LA DOCUMENTACIÓN SE PROPORCIONA "TAL CUAL" SIN GARANTÍAS NI CONDICIONES DE NINGUNA CLASE, NO GARANTIZA DECLARACIONES O GARANTÍAS EXPRESAS O IMPLÍCITAS, INCLUIDAS, A MERO TÍTULO ENUNCIATIVO, LAS GARANTÍAS IMPLÍCITAS DE COMERCIABILIDAD, IDONEIDAD PARA UN FIN DETERMINADO O NO VIOLACIÓN, A MENOS QUE TALES RENUNCIAS SEAN CONSIDERADAS NO VÁLIDAS SEGÚN LA LEY. SYMANTEC CORPORATION NO SERÁ RESPONSABLE DE NINGÚN DAÑO INCIDENTAL O CONSECUENTE RELACIONADO CON LA ENTREGA O EL USO DE ESTA DOCUMENTACIÓN. LA INFORMACIÓN CONTENIDA EN ESTA DOCUMENTACIÓN ESTÁ SUJETA A CAMBIOS SIN PREVIO AVISO.

La Documentación y el Software con licencia se consideran software informático comercial, como están definidos en el artículo 12.212 de las FAR, y están sujetos a derechos restringidos, como están definidos en el artículo 52.227-19 de las FAR, y "Software informático comercial: derechos restringidos" del artículo 227.7202 del Suplemento a las FAR, "Derechos del software informático comercial o Documentación de software comercial para equipos informáticos", según corresponda y cualquier regulación sucesora. Cualquier uso, modificación, edición de reproducción, ejecución, muestra o divulgación de la Documentación y el Software con licencia

por parte del Gobierno de los EE. UU. se realizará exclusivamente conforme a las condiciones del presente Acuerdo.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com/es/mx/

Soporte técnico

El Soporte técnico de Symantec mantiene centros de soporte global. El rol principal del soporte técnico es responder a las consultas específicas sobre funciones del producto y la funcionalidad. El grupo de soporte técnico también crea contenido para nuestra Base de conocimientos en línea. El grupo de soporte técnico funciona en conjunto con las otras áreas funcionales dentro de Symantec para contestar a sus preguntas a su debido tiempo. Por ejemplo, el grupo de soporte técnico trabaja con la ingeniería de productos y con Symantec Security Response para proporcionar los servicios de alertas y las actualizaciones de definiciones de virus.

Las ofertas del soporte de Symantec incluyen lo siguiente:

- Una variedad de opciones de soporte que le dan la flexibilidad para seleccionar la cantidad adecuada de servicio para cualquier tamaño de organización.
- Soporte telefónico o basado en Web que proporciona una respuesta rápida e información de última hora.
- Seguro de la actualización que entrega las actualizaciones de software
- Soporte global comprado en horas de oficina regionales o 24 horas al día, 7 días a la semana.
- Ofertas de servicios Premium que incluyen Servicios de Administración de cuentas.

Para obtener información sobre los servicios de soporte de Symantec, puede visitar nuestro sitio web en la siguiente dirección URL:

www.symantec.com/business/support/

Se entregarán los servicios de soporte según su acuerdo de soporte y la política empresarial actual del soporte técnico de la empresa.

Contacto con la asistencia técnica

Los clientes con un acuerdo de soporte actual pueden acceder a la información de asistencia técnica en la siguiente dirección:

www.symantec.com/business/support/

Antes de comunicarse con la asistencia técnica, asegúrese de que usted ha cumplido los requisitos del sistema que se enumeran en la documentación del producto. Asimismo, es necesario estar en el equipo en el cual ocurrió el problema en caso de que sea necesario replicarlo.

Cuando se comunica con la asistencia técnica, tenga la siguiente información disponible:

- Nivel de la versión del producto

- Información del hardware
- Memoria disponible, espacio libre en el disco e información de la NIC
- Sistema operativo
- Versión y nivel del parche
- Topología de redes
- Enrutador, puerta de enlace e información de la dirección IP
- Descripción del problema:
  - Mensajes de error y archivos de registro
  - Solución de problemas que fue realizada antes de contactar a Symantec
  - Cambios de configuración del software y cambios de la red recientes

Concesión de licencias y registro

Si el producto de Symantec requiere registro o una clave de licencia, acceda a nuestra página web de soporte técnico en la siguiente URL:

www.symantec.com/business/support/

Servicio al cliente

En la siguiente dirección encontrará información sobre el Servicio al cliente:

www.symantec.com/business/support/

El Servicio al cliente está disponible para brindarle asistencia con respecto a preguntas no técnicas, como los siguientes tipos de problemas:

- Cuestiones relacionadas con las licencias de productos o la serialización.
- Actualizaciones de registros de productos, como cambios de direcciones o nombres.
- Información general sobre productos (funciones, disponibilidad de idiomas, representantes locales).
- La última información sobre actualizaciones y mejoras de productos.
- Información acerca del seguro de actualización y los contratos de soporte.
- Información sobre los programas de compras de Symantec.
- Consejos sobre las opciones de soporte técnico de Symantec.
- Cuestiones previas a las ventas que no están relacionadas con lo técnico.
- Problemas relacionados con CD-ROM, DVD o manuales

Recursos para acuerdos de soporte

Si desea consultar a Symantec en relación con algún acuerdo de soporte existente, comuníquese con el equipo de administración de acuerdos de soporte de su región:

Asia Pacífico y Japón	customercare_apac@symantec.com
Europa, Oriente Medio y África	semea@symantec.com
Norteamérica y América Latina	supportsolutions@symantec.com

Contenido

Soporte técnico 4

Sección 1 Introducción a los componentes claves de IT Management Suite 23

Capítulo 1 Introducción a Symantec Management Platform 24

Acerca de Symantec Management Platform 24
Novedades de IT Management Suite 7.5 25
Componentes de Symantec Management Platform 28
Cómo funciona pcAnywhere Solution 29
Acerca de cómo agregar productos a la plataforma 30
Dónde se puede obtener información adicional 31

Capítulo 2 Introducción a Symantec Management Console 34

Acerca de Symantec Management Console 34
Acerca de las vistas de la consola 36
Acerca de la vista Equipos 36
Buscar un equipo y guardar la búsqueda como filtro 39
Acerca de la vista Software 41
Buscar software y guardar la búsqueda 42
Acerca de la ventana Catálogo de software 43
Acerca de la vista Trabajos o tareas 44
Acerca de la vista Políticas 44
Acerca de los operadores de búsqueda 45
Configuración de las vistas mejoradas 47
Acceso a Symantec Management Console 48
Acceso a documentación en Symantec Management Console 50
Acceder a la página Mi portal 50
Acceso a la página inicial de Administración de Notification Server 51
Personalización de Symantec Management Console 52

Personalización del menú de la consola 53
Adición de acciones definidas por el usuario en el menú contextual 55
Creación y modificación de vistas 57
Adición de nuevos elementos directamente en una vista 58
Creación y modificación de páginas del portal 59
Creación y modificación de elementos web 61
Cómo guardar elementos de la consola como archivos XML 63

Sección 2 Cómo configurar los servidores de Symantec Management Platform 65

Capítulo 3 Cómo configurar Notification Server 66

Acerca de Notification Server 66
Acerca de configurar Notification Server 67
Cómo configurar los valores de Notification Server 68
Configuración de procesamiento de Notification Server 69
Configuración del servidor de correo y las direcciones 72
Configuración del registro de mensajes de estado 72
Abrir el visor de registros 73
Configuración del servidor proxy 74
Configuración de las credenciales del punto de distribución 75
Cómo configurar los valores de Notification Server con el configurador de NS 75
Cómo configurar la base de datos de administración de configuración 76
Depuración de base de datos de administración de configuración 80
Almacenamiento del historial de datos de recursos en la CMDB 82

Capítulo 4 Configuración de seguridad 84

Acerca de la seguridad de Symantec Management Platform 84
Configuración de la seguridad de Symantec Management Platform 85
Creación y configuración de roles de seguridad 89
Asignación de privilegios a un rol de seguridad 93
Creación y configuración de las cuentas de usuario Symantec Management Platform 225
Cómo especificar los detalles generales de la cuenta de usuario de Symantec Management Platform 98
Configuración de credenciales para una cuenta de usuario de Symantec Management Platform 99

Adición de miembros a un rol de seguridad 101
Asignación de una cuenta de usuario de Symantec Management Platform a un rol de seguridad 102
Cómo agregar roles de seguridad como miembros de otros roles de seguridad 103
Asignación de permisos de seguridad a carpetas y elementos 103
Personalización de permisos de herencia 104
Roles de seguridad predefinidos 107
Tareas de administración de la seguridad de Symantec Management Platform 109
Configuración de la complejidad y del bloqueo de la contraseña 110
Cómo desbloquear las credenciales 113
Acceso al Administrador de roles de seguridad 113
Propiedad de una carpeta o elemento 115
Cómo administrar credenciales 115

Capítulo 5 Configuración de programaciones 117

Cómo Symantec Management Platform usa las programaciones 117
Componentes de una programación de Symantec Management Platform 119
Cómo administrar programaciones compartidas 122
Configuración de una programación 123
Visualización del calendario interno de programaciones de Notification Server 124

Capítulo 6 Configurar los sitios y los servidores de sitio 127

Acerca de los servicios de sitio 127
Acerca del mantenimiento del sitio 128
Administración de sitios 129
Administración de servidores de sitio 131
Cómo asignar un servidor de sitio a un sitio de forma manual 133
Cómo administrar agentes asignados de forma manual 134
Administración de subredes 135
Acerca de la configuración del servicio de sitio 138
Configuración de Package Service 139
Cómo establecer la configuración del servicio de tareas 139

Capítulo 7 Configuración de Package Server para Linux 141

Acerca de Package Server para Linux 141
Acerca de integrar al servidor web Apache con Package Server para Linux 142
Acerca de detectar el servidor web Apache 143
Requisitos para configurar Package Server y el servidor web Apache 145
Requisitos para configurar HTTPS y HTTP 146
Ejemplo de configuración de Package Server que usa el directorio web principal para los vínculos de Package Server 147
Ejemplo de la configuración de Package Server usando un alias para los vínculos de Package Server 150

Capítulo 8 Configuración de la jerarquía 153

Acerca de la jerarquía de Notification Server 153
Requisitos de la jerarquía 155
Implementar la jerarquía de Notification Server 156
Creación y administración de relaciones jerárquicas 157
Configurar una relación jerárquica entre dos equipos con Notification Server 161
Configurar la réplica de la jerarquía y las reglas de la réplica de la jerarquía 163
Cómo configurar una réplica de la jerarquía personalizada 165
Cómo anular la programación de réplica diferencial de jerarquía 167
Cómo replicar datos seleccionados manualmente 168
Configurar una política de automatización de jerarquía 168
Cómo ejecutar un informe de jerarquía 169
Cómo actualizar datos de resumen 170

Capítulo 9 Configuración de la replicación 172

Acerca de la replicación y las reglas de replicación 172
Requisitos de replicación 174
Configuración de las reglas de replicación 175

Capítulo 10 Cómo realizar una configuración por primera vez 177

Cómo realizar las tareas de configuración por primera vez 177
Detección de equipos 179

Iniciar Symantec Management Agent y los complementos de la solución 181
Opciones de configuración de agente y tareas 184
Recopilación de información de inventario 185
Programación de la administración de parches 187

Sección 3 Detectar los recursos en su red 189

Capítulo 11 Detección de equipos con Windows 190

Métodos de detección de recursos 190
Métodos de detección para equipos Windows 191
Cómo detectar equipos con la detección de recursos de dominio 192

Capítulo 12 Importación de recursos de Active Directory 197

Acerca de la importación de Microsoft Active Directory 197
Acerca de la importación de asociaciones de recursos 198
Importación de recursos mediante la importación de Microsoft Active Directory 199
Creación y modificación de reglas de importación de recursos 201
Programación de reglas de importación de recursos 204
Cómo configurar la programación de sincronización del directorio 205
Ejecución manual de reglas de importación de recursos 206

Capítulo 13 Detección de dispositivos de red 208

Acerca de Network Discovery 208
Detección de dispositivos de red 209
Cómo establecer la configuración de detección 210
Creación de tareas de Network Discovery con el asistente 212
Creación y modificación manual de tareas de Network Discovery 213
Cómo crear perfiles de conexión con Network Discovery 214
Creación o clonación de un perfil de conexión 215
Métodos para detectar dispositivos de red 216
Sobre seleccionar los intervalos de red para detectar 217
Visualización de dispositivos detectados en vistas organizativas 219
Visualización de informes de detección 219
Clasificación de dispositivos SNMP 220

Delegar tareas de Network Discovery a usuarios que no son administradores 221
Agregar usuarios que no sean administradores a roles de seguridad para realizar tareas de Network Discovery 224
Cómo habilitar los roles que no son de administrador para crear o ejecutar tareas de Network Discovery 226
Cómo conceder privilegios para crear credenciales y perfiles de conexión a los roles que no sean el de administrador 229
Concesión de acceso a roles que no sean de administrador al perfil de conexión predeterminado 230
Habilitación de roles que no sean los roles de seguridad predefinidos para crear y ejecutar tareas usando el asistente de Network Discovery 231
Cómo realizar un perfil de conexión de solo lectura 232
Importación de archivos MIB 233

Sección 4 Cómo instalar y configurar Symantec Management Agent 235

Capítulo 14 Introducción a Symantec Management Agent 236

Acerca de Symantec Management Agent 236
Acerca del registro de agente 237

Capítulo 15 Instalar Symantec Management Agent en los equipos cliente 238

Métodos para instalar Symantec Management Agent 238
Instalar Symantec Management Agent en equipos con Windows 240
Requisitos previos de instalación de Symantec Management Agent para Windows 242
Crear una política de registro de agente 243
Especificar Symantec Management Agent para la configuración de instalación de Windows 245
Cómo instalar Symantec Management Agent para Windows manualmente en modo push 246
Cómo instalar Symantec Management Agent para Windows con instalación manual en modo pull 247
Realizar una instalación programada de Symantec Management Agent para Windows 249
Visualización del informe de estado de la instalación 250
Ver y administrar el estado de registro del agente 251

Instalar Symantec Management Agent manualmente en equipos con UNIX, Linux y Mac 255
Cómo crear un archivo CSV para importar equipos con UNIX, Linux y Mac 256
Requisitos previos para la instalación de Symantec Management Agent para UNIX, Linux y Mac 258
Cómo especificar la configuración de instalación de Symantec Management Agent para UNIX, Linux y Mac 259
Cómo instalar Symantec Management Agent para UNIX, Linux y Mac manualmente en modo push 260
Cómo instalar Symantec Management Agent para UNIX, Linux y Mac manualmente en modo pull 264

Capítulo 16 Actualizar y desinstalar Symantec Management Agent 266

Métodos para actualizar Symantec Management Agent 266
Métodos para desinstalar Symantec Management Agent 267
Cómo configurar las políticas de actualización y de desinstalación de Symantec Management Agent 268
Acerca de la comunicación de agente de una versión anterior 272
Configuración del paquete de Symantec Management Agent 273
Cómo quitar Symantec Management Agent para Windows manualmente 274

Capítulo 17 Cómo configurar Symantec Management Agent 276

Cómo configurar Symantec Management Agent 276
Configuración de las opciones de configuración global de agente 277
Configuración de las opciones de configuración del agente de destino 278
Configuración de políticas de ventana de mantenimiento 280

Sección 5 Implementar la administración habilitada para la nube 283

Capítulo 18 Introducir la administración habilitada para la nube 284

Acerca de la administración habilitada para la nube 284

Capítulo 19 Preparar su entorno para la administración habilitada para la nube 287

Preparar su entorno para la administración habilitada para la nube 287
Configurar Notification Server para usar HTTPS 291
Cómo aplicar un certificado de una autoridad de certificación raíz a un equipo administrado 292
Cómo redireccionar Symantec Management Agent para usar HTTPS 295
Generar y aplicar el certificado de servidor de sitio para el acceso del agente habilitado para la nube 296
Configuración de un servidor de paquetes para publicar bases de código de paquetes de HTTPS 302
Configuración de sitios y servidores de sitio para servir a los agentes habilitados para la nube 304

Capítulo 20 Configurar la administración habilitada para la nube 307

Configurar la administración habilitada para la nube 307
Configuración de DefaultAppPool para usar el modo integrado de canalización administrada 310
Establecer la configuración del sitio web de IIS para el agente de administración habilitado para la nube 311
Acerca de la preparación del equipo de gateway de Internet 313
Descarga y ejecución del paquete de instalación del gateway de Internet 315
Configurar el gateway de Internet 317
Configurar la política de Configuración de administración habilitada para la nube 320
Cómo instalar Symantec Management Agent en un equipo desconectado 323

Capítulo 21 Realizar las tareas de administración habilitada para la nube 327

Tareas de mantenimiento y solución de problemas habilitadas para la nube 327
Cómo generar un certificado de cliente temporal 328
Cómo instalar un certificado temporal en un equipo administrado 331
Revocar un certificado de administración habilitada para la nube 332

Cómo forzar Symantec Management Agent para usar un gateway de Internet especificado 335
Hacer copia de seguridad de un gateway de Internet y restaurarlo 336
Visualización de informes de administración habilitada para la nube 338

Sección 6 Cómo administrar recursos de Symantec Management Platform 339

Capítulo 22 Configuración de la seguridad de recursos 340

Configuración de la seguridad de recursos 340
Crear y configurar una vista organizativa 343
Crear y rellenar una vista o grupo organizativo 343
Crear y configurar un grupo organizativo 344
Recursos de la visualización en un grupo organizativo 345
Configuración de la seguridad en un grupo organizativo 346
Consideraciones para el ámbito del recurso 348

Capítulo 23 Configuración de filtros y destinos de recursos 353

Acerca de los filtros de recursos 353
Creación o modificación de un filtro 354
Creación de un nuevo filtro 355
Modificación de un filtro existente 356
Selección del tipo de consulta del filtro 357
Cómo definir una consulta de recursos para un filtro 358
Cómo definir una consulta SQL para un filtro 360
Especifique las inclusiones y las exclusiones de filtro. 361
Actualización de la pertenencia a un filtro 363
Ejecución de acciones en recursos de filtros 364
Visualización de las dependencias de filtro 365
Acerca de los destinos de recursos 366
Programación de actualizaciones de pertenencia de recursos 367

Capítulo 24 Configuración de paquetes 370

Cómo cambiar la configuración de un paquete 370
Cómo actualizar los puntos de distribución de un paquete 371
Habilitación del acceso a un paquete en una ubicación UNC de origen 372
Cómo administrar programas del paquete 373

Capítulo 25 Uso de directivas 375

Acerca de las políticas de Symantec Management Platform 376
Acerca de las políticas basadas en el usuario 377
Cómo administrar las políticas de Symantec Management Platform 378
Aplicar una política usando arrastrar y soltar 378
Especificación de destinos de una política o tarea 379
Modificación de un destino de recursos 381
Cómo generar un destino de recursos 382
Cómo seleccionar un destino de recursos existente 383
Cómo guardar un destino de recursos con nombre 383
Cómo especificar reglas de filtro para los destinos de recursos 384
Cómo seleccionar los destinos de recursos con nombre 386
Cómo especificar una programación de política 387
Configurar las políticas de instalación, actualización y desinstalación del agente o complemento 389
Acerca de las políticas de automatización 391
Componentes principales de las políticas de automatización 392
Administración de políticas de automatización 393
Creación o modificación de políticas de automatización programadas 396
Creación o modificación de políticas de automatización basadas en mensajes 398
Especificación del origen de datos de políticas de automatización 401
Especificación de una acción de política de automatización 402
Seleccionar trabajo o tarea para la política de automatización 404
Creación y modificación de tareas de políticas de automatización 405

Capítulo 26 Usar las tareas y los trabajos 407

Acerca de la administración de tareas 407
Componentes de administración de tareas 409
Cómo Task Server usa el mecanismo de señal 410
Cuándo usar tareas, trabajos y políticas 412
Acerca de cómo ejecutar tareas en jerarquía 413
Secuenciación de tareas 416
Implementación de un Task Server 417
Cómo crear una tarea 418
Cómo crear un trabajo 418
Ejecutar un trabajo o una tarea usando arrastrar y soltar 420
Ejecución de un trabajo o una tarea 421

Volver a ejecutar una tarea con errores 422
Adición de una programación a una política, una tarea o un trabajo 424
Cómo ver el estado de tarea en Symantec Management Agent 425
Cómo consultar y editar permisos en un tipo de tarea 425
Creación de tareas para introducir o mostrar las propiedades de la tarea 426
Cómo limpiar datos de tarea 429
Limpiar datos de la versión de la tarea 429
Cómo cambiar la configuración de Client Task Agent 430
Acceder al Portal de trabajos y tareas 432

Capítulo 27 Uso del Administrador de recursos 433

Acerca de la administración de recursos 433
Acceso al Administrador de recursos 434
Visualización de datos de inventario para una clase de datos 435
Visualización de datos del evento para una clase de datos 436
Cómo agregar un recurso a un grupo organizativo 436
Tareas del Administrador de recursos 437

Capítulo 28 Cómo usar los informes de Notification Server 439

Acerca de los informes de Notification Server 439
Cómo ver y administrar datos de recursos con informes de Notification Server 440
Cómo extraer resultados del informe de Notification Server 441
Cómo ver los resultados del informe de Notification Server 443
Cómo usar los resultados del informe de Notification Server 444
Cómo guardar los resultados del informe de Notification Server como un archivo 446
Cómo crear un filtro estático a partir de resultados del informe de Notification Server 447
Cómo guardar los resultados del informe de Notification Server como una instantánea 448
Cómo guardar los resultados del informe de Notification Server como un elemento web 448

Capítulo 29 Cómo crear los informes personalizados de Notification Server 450

Componentes de un informe personalizado de Notification Server 450
Creación y modificación de informes personalizados de Notification Server 452
Cómo crear un informe personalizado de Notification Server 455
Cómo modificar un informe personalizado existente de Notification Server 456
Cómo definir una consulta de recursos para un informe personalizado 457
Cómo definir una consulta SQL para un informe personalizado 459
Definir parámetros y proveedores de valores para un informe personalizado 460
Cómo crear o modificar una vista de gráfico para un informe personalizado 462
Cómo crear o modificar una vista de cuadrícula para un informe personalizado 464
Cómo configurar acciones de examinación de niveles inferiores para un informe personalizado 465
Cómo especificar las propiedades avanzadas de un informe personalizado 468

Capítulo 30 Visualización de información del recurso 470

Acerca de los recursos 470
Cómo ver información de clase de datos del recurso 471
Cómo ver la información de tipo de asociación de recursos 471
Cómo ver la información de tipo de recurso 471

Sección 7 Cómo administrar datos de la CMDB con Data Connector 473

Capítulo 31 Introducción a Data Connector 474

Acerca de Data Connector 474
Cómo funciona Data Connector 475
Acciones que pueden llevarse a cabo con Data Connector 476

Capítulo 32 Realizar tareas de administración de datos 477

Cómo importar y exportar datos 477
Acerca de preprocesar datos antes de importar los datos 479
Cómo crear una definición de origen de datos 479
Crear una regla de transferencia de datos 480
Crear una llave de búsqueda del recurso 481
Cómo ejecutar una regla de transferencia de datos como tarea 482
Cómo ver resúmenes de transferencia de datos 483
Comprobación del estado de las reglas de la transferencia de datos 483
Crear una regla de CMDB para editar datos de CMDB 484
Cómo ejecutar una regla de CMDB como tarea 485
Cómo crear una clase de datos virtual 486
Configurar las opciones de depuración del registro detallado de Data Connector 487

Apéndice A Privilegios y permisos de seguridad 488

Categorías de privilegios de seguridad 489
Categorías de permisos de seguridad 491
Privilegios del perfil de conexión 492
Privilegios de administración 492
Privilegios del sistema 494
Privilegios de credenciales 496
Privilegios de directorio de flujo de trabajo 497
Privilegios de Symantec Management Console 497
Privilegios de Software Management 498
Privilegios del menú contextual 500
Menú contextual: Privilegios de muestras del conector 502
Privilegios de jerarquía 502
Privilegios de las acciones 503
Establecer privilegios de estados de los activos 505
Permisos de administración de recursos 505
Permisos del sistema 506
Permisos de Task Server 506
Permisos de informes 507
Permisos de políticas 507
Permisos de carpeta 507
Permisos de filtro 508
Permisos del perfil de conexión 508
Permisos de Credential Manager 509

Apéndice B Symantec Management Agent 510

Intervalos de actualización de datos recomendados de Symantec Management Agent 510
Comandos de solución de problemas de Symantec Management Agent para UNIX, Linux y Mac 511

Apéndice C Temas de referencia de administración habilitada para la nube 516

Herramientas de la línea de comandos de Notification Server 516
Configuraciones admitidas para los servidores de paquetes en un entorno mixto 517
Efectos de la funcionalidad Administración habilitada para la nube en el servidor de sitio 518
Scripts de administración del gateway de Internet 520
Acerca del equilibrio de carga del gateway de Internet 521
Parámetros del paquete de instalación del agente habilitado para la nube 522
Conmutadores de línea de comandos para la configuración de agentes habilitados para la nube 523

Apéndice D Configuración del informe personalizado 525

Página Edición de informes personalizada 526
Página Edición de informes personalizada: Ficha Origen de datos 527
Página Edición de informes personalizada: ficha Origen de datos, ficha Consulta 529
Página Edición de informes personalizada: ficha Origen de datos, ficha: Campos 532
Página Edición de informes personalizada: ficha Origen de datos, ficha Consulta con parámetros 533
Página Edición de informes personalizada: ficha Origen de datos, ficha Parámetros de consulta 534
Página Edición de informes personalizada: ficha Origen de datos, ficha: Expresiones de filtro 535
El informe personalizado edita la página: ficha Origen de datos : ficha Instantáneas de datos 535
Página Edición de informes personalizada: ficha Origen de datos,, ficha: Consulta resuelta 537
Página Edición de informes personalizada: ficha Origen de datos, ficha Resultados 538

Página Edición de informes personalizada: ficha Vistas para una vista de gráfico 539
Página Edición de informes personalizada: ficha Vistas para una vista de cuadrícula 542
Cuadro de diálogo Editar campos de origen 544
Cuadro de diálogo Edición de parámetro 546

Apéndice E Campos que admiten scripts para modificar las reglas de importación y exportación de recursos y las reglas de CMDB 548

Campos que admiten scripts para modificar las reglas de importación y exportación de recursos y las reglas de CMDB 548
Sintaxis de expresiones 549
Operadores de expresiones 550
Valores definidos por el usuario 550
Operadores de cadena 550
Caracteres comodín 551
Tipos de agregado 551
Funciones de expresiones 551

Apéndice F Avisos legales de otros fabricantes de Symantec™ Management Platform 7.5 555

Avisos legales de otros fabricantes 556
7-Zip 556
Apache HTTP Server 557
Apache Xerces C++ 560
Boost 564
Bouncy Castle 565
Curl 565
glibc 566
Libatomics_Ops 576
LibXML2 577
Makeself 577
Microsoft Anti-Cross Site Scripting Library 584
OpenPegasus 585
OpenSSL 0.9.8u 586
OpenSSL 0.9.8y 589
OpenSSL 1.0.1e 592
plists-cs 595
SQLite 595
Windows Template Library 'WTL' v8.0 595

Zlib 597

Índice 598

Sección 1

Introducción a los componentes claves de IT Management Suite

- Capítulo 1. Introducción a Symantec Management Platform
- Capítulo 2. Introducción a Symantec Management Console

Capítulo 1

Introducción a Symantec Management Platform

En este capítulo se incluyen los temas siguientes:

- Acerca de Symantec Management Platform
- Novedades de IT Management Suite 7.5
- Componentes de Symantec Management Platform
- Cómo funciona pcAnywhere Solution
- Acerca de cómo agregar productos a la plataforma
- Dónde se puede obtener información adicional

Acerca de Symantec Management Platform

Symantec Management Platform proporciona un conjunto de servicios que pueden aprovechar las soluciones relacionadas con TI. Las soluciones se integran en la plataforma y aprovechan los servicios que esta ofrece, como seguridad, informes, comunicaciones, distribución del paquete y datos de la Base de datos de la administración de configuración (CMDB). Debido a que las soluciones están en la misma plataforma, pueden compartir los servicios y los datos. Los datos compartidos son más útiles que aquellos que solamente están disponibles para una sola solución. Por ejemplo, una solución recopila datos sobre el software que está instalado en los equipos de la compañía y otra solución usa los datos para administrar licencias de software. Una tercera solución puede utilizar también estos datos para ayudarlo a actualizar el software. Esta integración tan estrecha entre las soluciones y la plataforma facilita el uso de diferentes soluciones debido a que trabajan en un entorno común y están administradas mediante una interfaz común.

La plataforma proporciona los siguientes servicios:

- Seguridad basada en roles
- Comunicaciones y administración de clientes
- Ejecución de tareas y políticas programadas o activadas por eventos
- Distribución e instalación de paquetes
- Elaboración de informes
- Administración centralizada mediante una interfaz única y común
- Base de datos de administración de configuración (CMDB)
- Software Management Framework

Cuando instala una solución o un conjunto de aplicaciones, también se instala la plataforma si no está ya instalada.

Ver "Componentes de Symantec Management Platform" en la página 28.

Ver "Cómo funciona pcAnywhere Solution" en la página 29.

Ver "Acerca de cómo agregar productos a la plataforma" en la página 30.

Ver "Novedades de IT Management Suite 7.5" en la página 25.

Novedades de IT Management Suite 7.5

En la versión 7.5 de IT Management Suite, se presentan las siguientes nuevas funciones:

Tabla 1-1 Lista de nuevas funciones

Función	Descripción
Mejoras generales	■ Los administradores notarán que el rendimiento de la consola es hasta 15 veces más rápido que en las versiones anteriores. ■ La nueva funcionalidad **Volver a ejecutar tarea** le permite volver a ejecutar las tareas en los equipos en los que falló una tarea. ■ La nueva página del folioscopio de Software Delivery le permite ver y usar la información de resumen sobre las tareas de Entrega rápida y las políticas de Managed Delivery en su entorno.

Función	Descripción
Administración habilitada para la nube (CEM)	Administración habilitada para la nube (CEM) le permite administrar los endpoints que viajan incluso cuando esos endpoints no se conectan a la red corporativa con VPN. Esta funcionalidad ayuda a mejorar la cobertura de la implementación de parches y software de sus empleados móviles y empleados que trabajan a distancia. CEM permite la comunicación completamente segura entre los endpoints en roaming y los Notification Servers en la red interna. Las soluciones y la funcionalidad siguientes se admiten mediante CEM: ■ Administración de tareas La Administración de tareas le permite ejecutar cualquier tipo de tarea en el modo CEM. Sin embargo, la conexión de señales a Task Server no se establece en el modo CEM y la ejecución inmediata de la tarea no está disponible. Las tareas pueden ejecutarse con hasta 60 minutos de retraso según la configuración predeterminada. Ejecutar Task Server en un equipo cliente habilitado para la nube y administrado en Internet no se admite y puede llevar a un comportamiento indeseable. ■ Inventory Solution Se admiten las funciones de inventario de hardware, inventario de software, inventario personalizado, inventario del servidor y medición de aplicaciones. CEM se admite en los equipos con Windows solamente. ■ Software Management Solution ■ Patch Management Solution
Registro de agente	Junto con la función de administración habilitada para la nube que le permite administrar los dispositivos que están fuera del firewall, la función de registro de agente fue agregada en IT Management Suite 7.5 para asegurarse que solamente los endpoints de confianza puedan comunicarse con Notification Server. La función de registro de agente requiere que un endpoint esté habilitado para comunicarse con Notification Server antes de que pueda ser administrado por este Notification Server.
Modo de comunicación de agente de una versión anterior (LAC)	El modo **Comunicación de agente de una versión anterior** (LAC) le permite controlar si los equipos que usan versiones anteriores de Symantec Management Agent pueden comunicarse con Notification Server 7.5 actualizado. Esta opción le permite actualizar los agentes en su entorno en fases en lugar de que se actualicen todos inmediatamente después de la actualización de Notification Server.

Función	Descripción
La lista de sistemas operativos admitidos se ha expandido.	El sistema operativo siguiente ahora se admite para la instalación de Symantec Management Platform y de sus componentes: ■ Windows Server 2008 R2 SP1 (de 64 bits) Las siguientes versiones de SQL Server ahora se admiten para la base de datos de administración de configuración (CMDB): ■ Microsoft SQL Server 2008 R2 SP1 ■ Microsoft SQL Server 2008 SP3 ■ Microsoft SQL Server 2012 Los sistemas operativos siguientes ahora se admiten para la instalación de Symantec Management Agent: ■ Windows 7 SP1 ■ Windows 8 ■ Windows Server 2008 R2 SP1 ■ Windows Server 2012 ■ Red Hat Enterprise Linux 5.7, 5.8, 6.2 y 6.3 **Nota:** Los sistemas operativos Windows 8 y Windows Server 2012 no se admiten para su uso como servidores de sitio.
Compatibilidad con Internet Explorer 10 (Modo de compatibilidad) en Portal de software	Portal de software de Software Management Solution ahora admite Internet Explorer 10 en el Modo de compatibilidad.
Se ha implementado un nuevo visor de registros.	Las siguientes características nuevas se introducen en el nuevo visor de registros: ■ Es posible cargar una gran cantidad de archivos de registro sin consumir demasiados recursos de su servidor. ■ Se ha simplificado el mecanismo del filtro y las definiciones del filtro se pueden guardar para su uso posterior. ■ Se introduce el mecanismo de marcadores. ■ Es posible realizar una búsqueda en los archivos de registro sin cargar los archivos de registro en visor de registros.
Se ha implementado la funcionalidad **SuppressReportAutorun**.	Cuando se habilita **SuppressReportAutorun** y se abre cualquier informe, el informe no se ejecuta de forma inmediata. Para ver los resultados del informe, es necesario hacer clic en **Actualizar**. De forma predeterminada, la funcionalidad **SuppressReportAutorun** está deshabilitada. Es posible habilitarla en **Configurador de NS**, en **Configuración básica > Interfaz de usuario > Informe > SuppressReportAutorun**.

Función	Descripción
Se quita la comprobación de la licencia de CMDB Solution.	La comprobación de licencia de CMDB Solution se ha quitado, lo que pone a CMDB Solution a disposición de todas las soluciones de Altiris como función. Es posible ahora instalar CMDB Solution como función de Inventory, Client Management Suite y Server Management Suite. Ya está instalada con Asset Management Suite, ServiceDesk e IT Management Suite. **Nota:** En una jerarquía, CMDB Solution debe instalarse en el Notification Server principal. No instale CMDB Solution en un Notification Server secundario.
Se quita componente de Altiris Out of Band Management.	En la versión IT Management Suite 7.5, el componente de Altiris Out of Band Management ya no está disponible. Si actualiza desde versiones anteriores de IT Management Suite, la utilidad **OOBRemover** quita los elementos de Administración OOB de Notification Server, de los servidores de sitio y de los equipos cliente.
Cambios en las notas de la versión de IT Management Suite 7.5 y la documentación de Symantec Management Platform 7.5.	En la versión IT Management Suite 7.5, la mayor parte de las notas de la versión específicas de la solución son rechazadas para las soluciones que son componentes de los conjuntos de aplicaciones siguientes: ■ Asset Management Suite ■ Client Management Suite ■ Server Management Suite Es posible encontrar la información de las notas de la versión específicas de la solución rechazadas en las notas de la versión específicas del conjunto de aplicaciones para los conjuntos respectivos. Para obtener más información, consulte el artículo siguiente: http://www.symantec.com/docs/DOC5702

Componentes de Symantec Management Platform

Tabla 1-2 Componentes de Symantec Management Platform

Componente	Descripción
Notification Server y Symantec Management Console	El servicio de Symantec Management Platform procesa eventos, facilita comunicaciones con equipos administrados y coordina el trabajo de otros servicios de dicha plataforma. La consola es la interfaz de usuario basada en Web del equipo con Notification Server que le permite administrar la plataforma y sus soluciones. Ver "Acerca de Notification Server" en la página 66. Ver "Acerca de Symantec Management Console" en la página 34.

Componente	Descripción
Base de datos de administración de configuración (CMDB)	Base de datos que almacena toda la información sobre los equipos administrados. Ver "Cómo configurar la base de datos de administración de configuración" en la página 76.
Servidores de sitio	Symantec Management Platform puede albergar varios tipos de componentes del middleware, tales como servicios de administración de paquetes, servicios de tareas y servicios de sitios de implementación. El nombre oficial para un componente de software intermedio es "servicio de sitio". Cualquier componente que aloje un servicio de sitio se conoce como un servidor de sitio. Los servidores de sitio pueden albergar uno o más de estos servicios. Ver "Acerca de los servicios de sitio" en la página 127.
Symantec Management Agent	Software que está instalado en un equipo para habilitar Notification Server con fines de supervisión y administración. Una vez que Symantec Management Agent está instalado, ese equipo se convierte en equipo administrado. Ver "Acerca de Symantec Management Agent" en la página 236.
Software Management Framework	Interfaz que le permite crear y administrar los recursos de software que se encuentran en el Catálogo de software. También le permite administrar los paquetes que están en la Biblioteca de software. La vista **Software** proporciona una ubicación central para iniciar las tareas relacionadas con el software que se realizan en su organización.
Informes	Una manera de recopilar la información automatizada. Es posible ver los informes en cualquier equipo administrado de Symantec Management Console. Ver "Cómo ver y administrar datos de recursos con informes de Notification Server" en la página 440.

Ver "Acerca de Symantec Management Platform" en la página 24.

Ver "Cómo funciona pcAnywhere Solution" en la página 29.

Cómo funciona pcAnywhere Solution

Symantec pcAnywhere Solution usa tecnología de control remoto. Puede conectarse a otro equipo o servidor y trabajar como si estuviera en frente de él. pcAnywhere Solution admite conexiones de red por medio de una red de área local (LAN), una red de área extensa (WAN) o Internet.

Puede ser útil comprender cierta terminología de pcAnywhere. Por ejemplo, el equipo cliente se llama equipo host porque alberga la conexión. El equipo del administrador se llama equipo remoto o consola. Esta terminología proviene de los entornos informáticos de "mainframe", donde un usuario remoto generalmente

se conecta a un servidor o a un equipo central. En pcAnywhere, el marco en la sesión se llama visor.

En la mayoría de los casos, los usuarios remotos inician la conexión. Ellos proporcionan la información necesaria para conectarse con el equipo host. El usuario remoto puede además seleccionar opciones para aumentar la seguridad u optimizar el rendimiento. Para establecer una conexión, el equipo host debe estar configurado para esperar las conexiones entrantes de pcAnywhere Solution.

pcAnywhere Solution incluye los elementos web de pcAnywhere para configuración, informes de Notification Server, la interfaz Administrador de pcAnywhere y el software pcAnywhere Solution.

pcAnywhere Solution proporciona las siguientes funciones:

- Seguridad basada en roles mediante las páginas de la consola
- Configuración de control del host administrado
- Registro de auditoría y elaboración de informes
- Seguridad y mecanismo de determinación del ámbito
- Integración con VNC y RDP

pcAnywhere Solution además incorpora las siguientes funciones de Notification Server:

- Task Server
- Jerarquía
- Políticas basadas en el usuario

Ver "Acerca de la jerarquía de Notification Server" en la página 153.

Ver "Acerca de la administración de tareas " en la página 407.

Ver "Acerca de las políticas basadas en el usuario" en la página 377.

Acerca de cómo agregar productos a la plataforma

Una amplia variedad de productos se puede ejecutar en Symantec Management Platform. Symantec y otras compañías proporcionan productos adicionales que se ejecutan en la plataforma. Por ejemplo, Symantec Client Management Suite ayuda a administrar los equipos endpoint y Symantec Server Management Suite ayuda a administrar los servidores.

Se usa Symantec Installation Manager para administrar la instalación de productos adicionales en la plataforma. En la página Instalar productos nuevos de Symantec Installation Manager, se puede ver una lista de productos disponibles. Es posible entonces instalar y evaluar fácilmente un producto. Los productos tienen

generalmente licencia de evaluación de 30 días. Es posible ver una lista de todos los productos instalados en la página Productos instalados de Symantec Installation Manager.

Cuando se compran productos, Symantec Installation Manager además administra las licencias. En la página Licencia de producto, se pueden aplicar licencias a los productos instalados y ver el estado de las licencias aplicadas.

Para obtener más información, consulte la *Guía de implementación y planificación de IT Management Suite*.

Dónde se puede obtener información adicional

Utilice los siguientes recursos de documentación para obtener más información sobre el producto y su utilización.

Tabla 1-3 Recursos de documentación

Documento	Descripción	Ubicación
Notas de la versión	Información sobre funciones nuevas y temas importantes.	La página **Productos admitidos de A a Z**, que está disponible en la siguiente URL: http://www.symantec.com/business/support/index?page=products Abra la página de soporte de su producto y, a continuación, en **Temas comunes**, haga clic en **Notas de la versión**.
Guía del usuario	Información sobre cómo utilizar este producto, incluida información técnica detallada e instrucciones para la ejecución de tareas comunes.	■ La Biblioteca de documentación, que está disponible en Symantec Management Console, en el menú **Ayuda**. ■ La página **Productos admitidos de A a Z**, que está disponible en la siguiente URL: http://www.symantec.com/business/support/index?page=products Abra la página de soporte de su producto y, a continuación, en **Temas comunes**, haga clic en **Documentación**.

Documento	Descripción	Ubicación
Ayuda	Información sobre cómo utilizar este producto, incluida información técnica detallada e instrucciones para la ejecución de tareas comunes. La Ayuda se encuentra disponible en el nivel de la solución y el conjunto de aplicaciones. Esta información se encuentra disponible en formato de ayuda HTML.	La Biblioteca de documentación, que está disponible en Symantec Management Console, en el menú **Ayuda**. La Ayuda contextual está disponible para la mayoría de las pantallas en Symantec Management Console. Puede abrir la Ayuda contextual de las siguientes maneras: ■ Haga clic en la página y, después, presione la tecla F1. ■ El comando Context, que está disponible en Symantec Management Console, en el menú **Ayuda**.

Además de la documentación del producto, puede utilizar los siguientes recursos para obtener más información sobre los productos de Symantec.

Tabla 1-4 Recursos de información de producto de Symantec

Recurso	Descripción	Ubicación
Base de conocimientos de soporte de SymWISE	Artículos, incidentes y temas relacionados con los productos de Symantec.	http://www.symantec.com/business/theme.jsp?themeid=support-knowledgebase

Recurso	Descripción	Ubicación
Symantec Connect	Un recurso en línea que contiene los foros, los artículos, los blogs, las descargas, los eventos, los videos, los grupos y las ideas para los usuarios de productos de Symantec.	http://www.symantec.com/connect/endpoint-management/forums/endpoint-management-documentation Esta es la lista de vínculos a los diversos grupos en Connect: ■ Implementación y creación de imágenes http://www.symantec.com/connect/groups/deployment-and-imaging ■ Detección e inventario http://www.symantec.com/connect/groups/discovery-and-inventory ■ Administrador de ITMS http://www.symantec.com/connect/groups/itms-administrator ■ Administración de Mac http://www.symantec.com/connect/groups/mac-management ■ Monitor Solution y estado del servidor http://www.symantec.com/connect/groups/monitor-solution-and-server-health ■ Administración de parches http://www.symantec.com/connect/groups/patch-management ■ Elaboración de informes http://www.symantec.com/connect/groups/reporting ■ ServiceDesk y flujo de trabajo http://www.symantec.com/connect/workflow-servicedesk ■ Administración de software http://www.symantec.com/connect/groups/software-management ■ Server Management http://www.symantec.com/connect/groups/server-management ■ Workspace Virtualization y Streaming http://www.symantec.com/connect/groups/workspace-virtualization-and-streaming

Capítulo 2

Introducción a Symantec Management Console

En este capítulo se incluyen los temas siguientes:

- Acerca de Symantec Management Console
- Acerca de las vistas de la consola
- Acceso a Symantec Management Console
- Acceso a documentación en Symantec Management Console
- Acceder a la página Mi portal
- Acceso a la página inicial de Administración de Notification Server
- Personalización de Symantec Management Console

Acerca de Symantec Management Console

Symantec Management Console (también conocida como "la consola") es una interfaz de usuario basada en Web. Es la herramienta principal para interactuar con Notification Server y sus componentes, y para administrar recursos.

Symantec Management Console se divide en las siguientes áreas:

Título

La parte principal de la consola que incluye lo siguiente:

- Menús, que permiten acceder a las páginas de la consola, y cuadros de diálogo, que proporcionan funciones de administración de Notification Server. Las soluciones de Symantec que están instaladas en el sistema pueden agregar nuevos elementos al menú.
- Cuadro Buscar, que permite buscar los datos de recursos para los recursos que desee. Cuando se realiza una búsqueda, aparece un panel de búsqueda en la parte inferior donde se introduce la búsqueda.
- Una barra de ruta de navegación que muestra la ruta del menú de la página mostrada.

Área de contenido

La parte de la consola que está debajo del título puede mostrar lo siguiente:

- Ver
  Una vista compuesta por una vista de árbol y el panel de contenido. La vista de árbol, que se encuentra en el panel izquierdo, muestra el orden jerárquico de los elementos que se pueden seleccionar y utilizar. El panel de contenido, que se encuentra en el panel derecho, muestra páginas basadas en selecciones de la vista de árbol.
- Página del portal
  La página del portal muestra una colección de varios fragmentos de información que contiene el componente Web part. Notification Server incluye las páginas del portal predefinidas, además de otras páginas del portal que pueden estar incluidas con soluciones. También puede crear sus propias páginas del portal.
- Página completa
  Una página completa tiene un único panel de contenido sin vista de árbol.

Algunas páginas de consolas admiten la personalización, que es la capacidad de que una página de consola conserve el estado de sus controles por usuario. Por ejemplo, un día el usuario A abre una página de filtro y, para acomodarla según su gusto, reordena las columnas de la cuadrícula. Mientras tanto, el usuario B abre la misma página, pero deja las hojas de la cuadrícula con la configuración predeterminada. Al día siguiente, cuando los usuarios abren la página de filtro, el usuario A la ve como la configuró el día anterior. El usuario B aún tiene la vista predeterminada como la dejó el día anterior.

La personalización se aplica a las páginas de elaboración de informes y de filtro, y al estado del árbol de navegación de las páginas de vista. Además, la página Mi portal se personaliza para cada usuario.

Acerca de las vistas de la consola

Una vista es un diseño de dos paneles con un árbol de navegación en el panel izquierdo y el contenido en el panel derecho. El árbol de navegación contiene vínculos a los elementos de Symantec Management Console y permite agrupar los elementos de diferentes partes de la consola en una estructura adecuada. Un elemento puede aparecer varias veces en una vista y en cualquier cantidad de vistas. Una vista puede incluir carpetas, vínculos de elementos y vínculos web. La Plataforma de administración Symantec y las soluciones incluyen las vistas predefinidas que se pueden modificar y ampliar según sea necesario. También puede crear sus propias vistas.

Ver "Creación y modificación de vistas" en la página 57.

Ver "Adición de nuevos elementos directamente en una vista" en la página 58.

Las vistas permiten organizar a las funciones de la solución y la Plataforma de administración Symantec y acceder a ellas. Es conveniente configurar las vistas para reflejar la funcionalidad que brinda una solución o una función, o para proporcionar a los usuarios un rol específico con acceso a ciertas tareas.

La estructura de árbol de navegación predeterminada que se puede ver en el panel izquierdo es la estructura real de la carpeta. Cada elemento aparece solamente una vez en la estructura real. Las carpetas de una vista pueden ser carpetas virtuales, las cuales no existen en la estructura real, o tal vez sean vínculos a las carpetas reales. Un vínculo a una carpeta real incluye todo lo que contiene esa carpeta. Si algunos elementos nuevos se agregan a la estructura real de esa carpeta, se incluyen automáticamente en la vista. No es posible excluir de una vista elementos que se encuentren en una carpeta, pero sí se pueden eliminar de la vista. Esto rompe el vínculo entre la vista y el elemento: no elimina el elemento real.

La seguridad se aplica a las vistas, de forma que lo que se ve depende de los privilegios de seguridad y los permisos. Para tener un privilegio o un permiso en una carpeta de una vista, éste se debe establecer directamente en la vista y en la carpeta real. Es posible ver solamente algunos elementos en una vista y que otros usuarios vean más o menos.

Acerca de la vista Equipos

Nota: Es necesario tener uno de los siguientes productos instalados para ver esta página: Deployment Solution (producto independiente), IT Management Suite, Server Management Suite o Client Management Suite.

Para acceder a la vista mejorada **Equipos**, en Symantec Management Console, haga clic en **Administrar > Equipos**.

La vista **Equipos** ofrece dos maneras de mirar los equipos en su entorno, la vista individual y la vista de resumen.

Nota: Es posible cambiar entre estas vistas haciendo clic en las flechas dobles (>> o <<) ubicadas a la derecha del título **Equipos**.

Vista individual

La vista individual le da detalles sobre un equipo específico. Es posible especificar este equipo en el panel de navegación ubicado a la izquierda o en el cuadro de búsqueda del panel de **lista**.

Tabla 2-1 Vista individual

Panel de navegación (Contiene las búsquedas guardadas y las vistas y grupos organizativos)	Panel de lista (Muestra los equipos de la búsqueda guardada o la vista o grupo organizativos seleccionados)	Panel de detalles (Muestra detalles de inventario sobre los equipos seleccionados)
Equipos **Búsquedas guardadas** ■ Nuevos equipos ■ Agente instalado ■ <Definido por el usuario> **Vistas de todos los equipos** ■ Todos los equipos ■ Máquina virtual Hojas: ■ **Equipos** ■ **Trabajos o tareas** ■ **Políticas** ■ **Software**	Campo de búsqueda Resultados de la búsqueda	Páginas del folioscopio: ■ General ■ Identificación ■ Detalles de Symantec Management Agent (necesita un agente instalado) ■ Hardware ■ Red ■ Unidades ■ Módulos de memoria ■ Correcciones de Microsoft ■ Programas con licencia Hojas ■ Trabajos o tareas ■ Políticas ■ Software

Vista de resumen

La vista de resumen agrega un folioscopio con tres páginas que proporciona información útil sobre las entregas de software, los fabricantes y los sistemas operativos en su entorno. La selección en el panel de navegación cambia los resultados en el panel resumen y el panel de lista. Hacer clic en un gráfico o un elemento de la leyenda dentro de las páginas del folioscopio restringe aún más el resultado. Puede agregar más criterios de búsqueda en la búsqueda avanzada.

Es posible cambiar entre las páginas del folioscopio haciendo clic en los vínculos de las páginas del folioscopio.

Tabla 2-2 Vista de resumen

Panel de navegación **(Contiene las búsquedas guardadas y las vistas y grupos organizativos)**	**Panel de resumen** **(Contiene un folioscopio con 3 páginas)**	**Panel de lista** **(Muestra los equipos de la búsqueda guardada o la vista o grupo organizativos seleccionados)**
Equipos	■ Entregas de software ■ Fabricantes ■ Sistemas operativos	Campo de búsqueda
Búsquedas guardadas ■ Nuevos equipos ■ Agente instalado ■ <Definido por el usuario>		Resultados de la búsqueda
Vista de todos los equipos ■ Todos los equipos ■ Máquina virtual		
Hojas ■ Equipos ■ Trabajos o tareas ■ Políticas ■ Software		

La vista **Equipos** le permite realizar las siguientes tareas:

- Busque equipos y guarde los resultados de la búsqueda para volver a utilizarlos como filtro personalizado para buscar equipos con trabajos, tareas, políticas o entrega de software.

Ver "Buscar un equipo y guardar la búsqueda como filtro" en la página 39.

- Cree y administre vistas y grupos organizativos.
  Ver "Crear y rellenar una vista o grupo organizativo" en la página 343.
- Arrastre y suelte los equipos en las vistas y los grupos organizativos.
  Ver "Crear y rellenar una vista o grupo organizativo" en la página 343.
- Vea información de resumen sobre las políticas de implementación administrada y las tareas de Entrega rápida, y actúe en función de dicha información
  Ver "Volver a ejecutar una tarea con errores" en la página 422.
- Consulte la información de resumen para obtener datos sobre los fabricantes de hardware y los sistemas operativos

Buscar un equipo y guardar la búsqueda como filtro

En la vista **Equipos**, se puede buscar un equipo o a un grupo específico de equipos aplicando o modificando una búsqueda guardada predefinida. Una búsqueda guardada es un filtro especial que muestra una lista dinámica de equipos que cumplen con los criterios del filtro. Es posible también crear una búsqueda guardada totalmente nueva.

Ver "Acerca de la vista Equipos " en la página 36.

La lista **Todos los equipos** es el punto de partida que muestra todos los equipos y todas las búsquedas guardadas.

Para buscar un equipo y guardar la búsqueda como filtro

1. En Symantec Management Console, en el menú **Administrar**, haga clic en **Equipos**.
2. En el panel de lista, en el campo de búsqueda, escriba todo o parte de un nombre de equipo.

Nombre completo	Escriba el nombre completo de un equipo o de un grupo específico de equipos que desee encontrar.
Nombre parcial	Escriba un nombre parcial si desea que su búsqueda devuelva todos los equipos que contengan una cadena de texto específica en cualquier lugar del nombre. Para ver todos los equipos con un prefijo de ubicación, como India, puede escribir **Ind**. Los resultados de búsqueda muestran todos los equipos que contienen la cadena.

3 (Opcional) Para usar las funciones de búsqueda avanzada, haga clic en la flecha hacia abajo al lado del campo de búsqueda y después seleccione el criterio de búsqueda que desee aplicar.

Ver "Acerca de los operadores de búsqueda" en la página 45.

4 (Opcional) Para seleccionar varios criterios de búsqueda, haga clic la flecha hacia abajo ubicada al lado de la lista desplegable **Agregar criterios de búsqueda**, seleccione un criterio y después repita el paso para agregar otros criterios.

Para quitar un criterio de búsqueda, deje el campo vacío.

5 (Opcional) Si los criterios que desea usar no se detallan en la lista desplegable de la búsqueda avanzada, cree criterios de búsqueda personalizados. Para crear un criterio de búsqueda personalizado, haga lo siguiente:

- En el panel de lista, haga clic en la flecha hacia abajo al lado del campo de búsqueda.
- En la lista desplegable **Agregar criterios de búsqueda**, haga clic en **Incorporar criterios personalizados**.
- En el cuadro de diálogo **Agregar criterios de búsqueda**, seleccione las clases de datos y las columnas que desee usar para los criterios de búsqueda.
  Tenga en cuenta que seleccionar columnas rellena los criterios de búsqueda en la lista desplegable y hace que los criterios adicionales estén disponibles como parte de su búsqueda.
- Haga clic en **Aceptar**.

6 Para guardar la búsqueda, haga clic en el icono de guardado en el área de búsqueda avanzada.

Tenga en cuenta que cualquier campo que no contenga un valor se omite en la consulta y no se guarda cuando se guarda la búsqueda.

7 En el cuadro de diálogo **Guardar búsqueda**, en el campo **Nombre**, escriba un nombre y haga clic en **Aceptar**.

La búsqueda guardada aparece en **Búsquedas guardadas** en el panel de navegación y queda disponible para que la reutilice.

8 (Opcional) Si usa una búsqueda guardada solamente como filtro para buscar trabajos, tareas o políticas y no desea que aparezca en el panel de navegación, puede ocultarla. Para ocultar la búsqueda guardada, haga lo siguiente:

- Haga clic con el botón derecho en **Búsquedas guardadas** y después haga clic en **Administrar búsquedas guardadas**.

- En el cuadro de diálogo **Administrar búsquedas guardadas**, anule la selección del cuadro ubicado al lado de la búsqueda que no desea que se muestre.
- Haga clic en **Cerrar**.

Video: Para obtener más información acerca de cómo crear búsquedas guardadas avanzadas en las vistas mejoradas, consulte Video sobre creación de búsquedas guardadas avanzadas en las vistas mejoradas de la consola en Symantec Connect.

Acerca de la vista Software

Nota: Es necesario tener uno de los siguientes conjuntos de aplicaciones o soluciones instalados para ver esta página: Deployment Solution (producto independiente), IT Management Suite, Server Management Suite o Client Management Suite.

Para acceder a la vista mejorada **Software**, en Symantec Management Console, haga clic en **Administrar > Software**.

La vista **Software** ofrece tres paneles: panel de navegación a la izquierda, una lista de software y de un panel del campo de búsqueda en el centro y un panel de contenido a la derecha. El panel de navegación contiene las búsquedas guardadas. El panel de lista muestra los elementos del software de la búsqueda guardada seleccionada. El panel de contenido muestra los detalles sobre el software que se selecciona.

La vista **Software** permite realizar las siguientes tareas:

- Buscar el software por nombre, fabricante u otros criterios.
  Ver "Buscar software y guardar la búsqueda" en la página 42.
- Administrar productos de software.
- Instalar software usando arrastrar y soltar.
- Administrar licencias de software.
- Realizar un seguimiento del uso del software y las licencias.

Video: Para obtener más información acerca de administrar el software en vistas mejoradas, consulte Video sobre importar software con vistas mejoradas de la consola, Video sobre administrar software importado con vistas mejoradas de la consola y Video sobre implementar software importado con vistas mejoradas de la consola en Symantec Connect.

Buscar software y guardar la búsqueda

En la vista mejorada de **Software**, los resultados de búsqueda que aparecen en el panel de lista no se filtran de forma automática. Es posible usar las funciones de búsqueda y búsqueda avanzada para restringir y para perfeccionar su lista, hasta que el panel de lista contenga el software específico.

Ver "Acerca de la vista Software " en la página 41.

Es posible guardar las búsquedas personalizadas del software y reutilizarlas más tarde. Las búsquedas guardadas aparecen en el panel de navegación, en el subpanel **Software instalado**. Es posible entonces usar búsquedas guardadas como filtros para buscar software para tareas, trabajos y políticas. Puede también usar búsquedas guardadas para entregar software a los equipos o a grupos específicos de equipos.

Para buscar un software específico y guardar la búsqueda

1. En Symantec Management Console, en el menú **Administrar**, haga clic en **Software**.
2. En el panel de navegación, haga clic en una búsqueda guardada que desee usar como punto de partida de su búsqueda.
3. En el panel de lista, en el campo de búsqueda, escriba los criterios de búsqueda.
4. (Opcional) Para usar las funciones de búsqueda avanzada, haga clic en la flecha hacia abajo al lado del campo de búsqueda y después seleccione el criterio de búsqueda que desee aplicar.

   Ver "Acerca de los operadores de búsqueda" en la página 45.
5. (Opcional) Para seleccionar varios criterios de búsqueda, haga clic la flecha hacia abajo ubicada al lado de la lista desplegable de los criterios de búsqueda, seleccione un criterio y después repita el paso para agregar otros criterios.
6. (Opcional) Si los criterios que desea usar no se detallan en la lista desplegable de la búsqueda avanzada, cree criterios de búsqueda personalizados. Para crear un criterio de búsqueda personalizado, haga lo siguiente:
   - En la lista desplegable **Agregar criterios de búsqueda**, haga clic en **Incorporar criterios personalizados**.
   - En el cuadro de diálogo **Agregar criterios de búsqueda**, seleccione las clases de datos y las columnas que desee usar para los criterios de búsqueda.

     Tenga en cuenta que seleccionar columnas rellena los criterios de búsqueda en la lista desplegable y hace que los criterios adicionales estén disponibles como parte de su búsqueda.

- Haga clic en **Aceptar**.

7 Para guardar la búsqueda, haga clic en el icono de guardado en el área de búsqueda avanzada.

Tenga en cuenta que cualquier campo que no contenga un valor se omite en la consulta y no se guarda cuando se guarda la búsqueda.

8 En el cuadro de diálogo **Guardar búsqueda**, en el campo **Nombre**, escriba un nombre y haga clic en **Aceptar**.

La búsqueda guardada aparece en **Software instalado** en el panel de navegación y está disponible para que se reutilice.

9 (Opcional) Si usa una búsqueda guardada solamente como filtro para buscar trabajos, tareas o políticas y no desea que aparezca en el panel de navegación, puede ocultarla. Para ocultar la búsqueda guardada, haga lo siguiente:

- Haga clic con el botón derecho en **Software instalado** y después haga clic en **Administrar búsquedas guardadas**.
- En el cuadro de diálogo **Administrar búsquedas guardadas**, anule la selección del cuadro ubicado al lado de la búsqueda que no desea que se muestre.
- Haga clic en **Cerrar**.

Acerca de la ventana Catálogo de software

Nota: Es necesario tener uno de los siguientes conjuntos de aplicaciones o soluciones instalados para ver esta página: Deployment Solution (producto independiente), IT Management Suite, Server Management Suite o Client Management Suite.

La ventana **Catálogo de software** aparece dentro de la vista **Software**.

Para acceder a la ventana **Catálogo de software**, en Symantec Management Console, haga clic en **Administrar > Catálogo de software**. Es posible también ir a **Administrar > Software**, hacer clic con el botón derecho en **Software instalado** y, después, hacer clic en **Administrar catálogo de software**.

Ver "Acerca de la vista Software " en la página 41.

En la ventana **Catálogo de software**, se pueden realizar las tareas de administración de software siguientes:

- Importar o agregar nuevos componentes de software y productos de software. Es posible importar el software incluso si no se encuentra en el inventario.

- Agregue el software recientemente detectado o indefinido que se propone administrar a su lista de software administrado.
- Mueva el software recientemente detectado o indefinido que usted no se propone administrar a su lista de software no administrado.
- Mover los productos de software de una lista a otra a medida que sus necesidades cambian.
- Eliminar un producto de software. Esta acción cancela la asociación entre los componentes de software y los paquetes a través de los cuales fueron entregados. Cuando se elimina un producto de software, sus componentes se detallan de nuevo en el panel **Software recientemente detectado/indefinido**.

Acerca de la vista Trabajos o tareas

Nota: Es necesario tener uno de los siguientes conjuntos de aplicaciones o soluciones instalados para ver esta vista: Deployment Solution (producto independiente), IT Management Suite, Server Management Suite o Client Management Suite.

Para acceder a la vista **Trabajos o tareas**, en Symantec Management Console, haga clic en **Administrar > Tareas y trabajos**.

La vista **Trabajos o tareas** le permite ver y trabajar con todos los trabajos y las tareas disponibles. Por ejemplo, puede ejecutar trabajos y las tareas arrastrándolos y soltándolos en uno o más equipos. Puede también usar la opción **Ejecución rápida** para señalar un trabajo o una tarea sin explorar los niveles inferiores manualmente.

Ver "Ejecutar un trabajo o una tarea usando arrastrar y soltar" en la página 420.

Ver "Especificación de destinos de una política o tarea" en la página 379.

Acerca de la vista Políticas

Nota: Es necesario tener uno de los siguientes conjuntos de aplicaciones o soluciones instalados para ver esta página: Deployment Solution (producto independiente), IT Management Suite, Server Management Suite o Client Management Suite.

Para acceder a la vista mejorada **Políticas**, en Symantec Management Console, haga clic en **Administrar > Políticas**.

La vista mejorada **Políticas** le permite ver todas las políticas disponibles y trabajar con ellas. Puede realizar todas las funciones comunes de aplicación de reglas y reparación en los equipos. Es posible configurar las programaciones de comprobación de compatibilidad y activar las políticas. Es posible poner en marcha las políticas arrastrándolas y soltándolas en uno o más equipos. Puede también usar la opción **Aplicar rápidamente en** para señalar una política sin explorar los niveles inferiores manualmente.

Ver "Aplicar una política usando arrastrar y soltar" en la página 378.

Ver "Especificación de destinos de una política o tarea" en la página 379.

Acerca de los operadores de búsqueda

Es posible usar los operadores de búsqueda para estrechar los resultados cuando se busca un elemento específico o un grupo de elementos.

Ver "Buscar un equipo y guardar la búsqueda como filtro" en la página 39.

Ver "Buscar software y guardar la búsqueda" en la página 42.

Las condiciones de búsqueda generales siguientes se aplican:

- Las comillas limitan su búsqueda a una coincidencia exacta.
  “Windows XP” = equipos que ejecutan **COINCIDENCIA EXACTA** Windows XP.
  “Adobe Acrobat” = equipos que ejecutan **COINCIDENCIA EXACTA** Adobe Acrobat.
- La omisión de comillas permite la coincidencia del texto de búsqueda en cualquier lugar de una cadena.
  Windows XP = equipos que se ejecutan **COMO** Windows XP en cualquier lugar del nombre.
  Adobe Acrobat = equipos que se ejecutan **COMO** Adobe Acrobat en cualquier lugar del nombre.

Tabla 2-3 Busque los operadores que se pueden usar para expresar diversos argumentos

Argumento	Símbolo	Descripción
O	Símbolo de barra vertical (|).	Este operador no necesita espacios iniciales. Cuando se busca un equipo, los ejemplos de uso son los siguientes: ■ **Windows|XP** = equipos que ejecutan **COMO** Windows **O COMO** XP ■ **XP|2000|2003** = equipos que ejecutan **COMO** XP **O COMO** 2000 **O COMO** 2003 Cuando se busca un software, el ejemplo de uso está es el siguiente: ■ **Adobe|Microsoft** = fabricante de software **COMO** Adobe **O COMO** Microsoft
Y, Agrega o Incluir	Signo más (+).	Este operador no necesita un espacio inicial. Cuando se busca un equipo, los ejemplos de uso son los siguientes: ■ **Windows+XP** = equipos que ejecutan **COMO** Windows **Y** XP ■ **Windows+2008** = equipos que ejecutan **COMO** Windows **Y** 2008 Cuando se busca un software, el ejemplo de uso está es el siguiente: ■ **Adobe+Microsoft** = fabricante de software **COMO** Adobe **Y** Microsoft
No, el menos o no incluye	Signo menos (-).	Este operador necesita un espacio inicial. Si inserta un signo menos sin un espacio inicial, no se interpreta como operador. Como práctica recomendada, comience con el grupo general dentro del cual desee buscar y después inserte el texto de exclusión. Cuando se busca un equipo, los ejemplos de uso son los siguientes: ■ **Windows** [espacio] **-XP** = equipos que ejecutan Windows **NO COMO** XP ■ **Windows Server** [espacio] **-2003** = equipos que ejecutan Windows Server **NO COMO** 2003 Los ejemplos siguientes asumen que sus equipos tienen nombres con números, como equipo-1, equipo-12, equipo-27, equipo-125, equipo-218, equipo-243 y equipo-321: ■ **equipo-** [espacio] **-1** = equipos con nombre equipo- **NO COMO** 1, 12, 125, 218, 321 ■ **equipo-** [espacio] **-1** = equipos con nombre equipo- **NO COMO** 27, 218, 321 Cuando se busca un software, el ejemplo de uso está es el siguiente: ■ **-Adobe -Microsoft** = fabricante de software **NO COMO** Adobe y **NO COMO** Microsoft

Configuración de las vistas mejoradas

Las vistas mejoradas en Symantec Management Console permiten configurar valores específicos. Es posible configurar los campos de búsqueda específica de modo que se puedan ver los resultados a medida que escribe el parámetro. Es posible configurar estos mismos campos de búsqueda de modo que pueda verlos resultados después de presionar **Intro**. Es posible configurar las vistas mejoradas para usar IME (Input Method Editor), de modo que pueda especificar los caracteres de doble byte en estas vistas. También puede configurar el número de equipos y software que aparece en la lista de resultados. Si administra un gran número de equipos, esta configuración puede mejorar el tiempo de carga.

Para configurar los valores de las vistas mejoradas

1. En **Symantec Management Console**, en el menú **Configuración**, haga clic en **Consola > Vistas mejoradas**.
2. En el cuadro de diálogo **Configuración de vistas mejoradas**, configure los valores siguientes:

Buscar	**Mientras escribe** : esta opción permite considerar los resultados a medida que escribe los requisitos en el campo de búsqueda. La configuración predeterminada es **A medida que escribe**. **Después de presionar Intro** : esta opción solo permite considerar los resultados después que se escriben los requisitos en el campo de búsqueda y presiona **Intro**. Estas opciones de búsqueda afectan los campos de búsqueda siguientes: ■ Vista **Equipos**, campo de búsqueda del panel central, que incluye todas las búsquedas guardadas y filtradas ■ Vista **Software**, campo de búsqueda del panel central, que incluye todas las búsquedas guardadas y filtradas
Permitir IME (Input Method Editor) para escribir caracteres de idioma de doble byte	Activa la compatibilidad con IME para vistas mejoradas y el portal Configuración por primera vez. Cuando se comprueba esta opción, puede usar IME para especificar los caracteres de doble byte en estas páginas.

Limite las listas de resultados por equipo y software a	Limita el número de equipos o software que pueden aparecer en una lista de resultados. Si el entorno tiene una jerarquía con los miles de equipos, las listas pueden tardar en cargarse y puede incluso agotarse el tiempo de espera. Este límite establece cuántas filas debe devolver la consulta. La configuración predeterminada es 20 000, pero puede reducir esta configuración para mejorar los tiempos de carga. Si hay filas adicionales, la fila más actual indica que hay más registros y permite cargarlos.

3 Haga clic en **Aceptar**.

Acceso a Symantec Management Console

A Symantec Management Console (también conocida como “la consola”) se puede acceder desde el equipo que está ejecutando Notification Server o de forma remota. Una conexión remota requiere que el equipo remoto tenga acceso al equipo con Notification Server y que se ejecute una versión admitida de Microsoft Windows y de Microsoft Internet Explorer. Gracias a que la consola está basada en un explorador web, no es necesario instalar ningún software especial para usarla.

Ver "Acerca de Symantec Management Console" en la página 34.

Para acceder a la consola, es necesario contar con uno o más roles de seguridad de Notification Server.

Ver "Acerca de la seguridad de Symantec Management Platform" en la página 84.

Nota: Symantec Management Platform admite autenticación NTLM para conexiones remotas. Esto permite acceder a Symantec Management Console desde un equipo remoto sin tener que introducir un nombre de usuario y una contraseña (a veces denominado “inicio de sesión único” en la consola). Debe iniciar sesión en el equipo remoto con una cuenta de Symantec Management Platform y es necesario usar el nombre de dominio completo (FQDN) para el nombre de Notification Server

Si se le solicita un nombre de usuario y una contraseña cuando se conecta a Symantec Management Console, es posible que deba agregar el nombre de Notification Server (FQDN) a la zona de sitios de confianza del equipo remoto. Es posible hacer esto mediante el Panel de control, en el cuadro de diálogo Propiedades de Internet, en la ficha Seguridad.

La consola admite Microsoft Internet Explorer de 32 bits 7.0. Todos los controles ActiveX que se usan son de 32 bits, de forma que los navegadores de 64 bits no se admiten. Si se abre la consola con un explorador no admitido, aparece un mensaje en la línea superior. El mensaje advierte que no se admite el explorador y que es posible que algunas funciones no estén disponibles. El uso de exploradores no admitidos es responsabilidad del usuario.

Deben instalarse algunos controles ActiveX para permitir que la consola funcione correctamente. Es necesario tener una cuenta de administrador en el equipo de la consola o que el equipo de soporte de TI instale los controles ActiveX adecuados.

Nota: Si experimenta problemas, como páginas de consolas que muestran mensajes de error, datos que se pierden o controles de la UI con comportamiento poco común, compruebe que el nombre de Notification Server esté especificado correctamente. El nombre de Notification Server solamente puede contener caracteres alfanuméricos. Los caracteres especiales no están permitidos, ni siquiera el carácter de subrayado.

Para acceder localmente a Symantec Management Console

- En el equipo local, en el menú **Inicio**, haga clic en **Todos los programas > Symantec > Symantec Management Console**.

Para acceder remotamente a Symantec Management Console

1. En un equipo remoto, abra Internet Explorer y vaya a la dirección URL siguiente:

   http://*Nombre de Notification Server*/altiris/console

   El nombre de Notification Server debe ser el nombre de dominio completo. De ser necesario, se puede utilizar HTTPS. Si Notification Server no está en el puerto 80, es necesario incluir el número de puerto adecuado después del nombre de Notification Server.

2. Si ha iniciado sesión en el equipo remoto con una cuenta que no sea la de Symantec Management Platform, se le pedirá el nombre de usuario y la contraseña.

   Si ha iniciado sesión en el equipo remoto con una cuenta de Symantec Management Platform, la función Inicio de sesión único la administra automáticamente. Si aparece la solicitud, es posible que deba agregar el nombre de Notification Server (FQDN) a la zona de sitios de confianza del equipo remoto.

Acceso a documentación en Symantec Management Console

Hay dos maneras para acceder a la documentación desde Symantec Management Console: ayuda contextual y la biblioteca de documentación. La Ayuda contextual permite acceder a información específica de la ubicación (página, cuadro de diálogo o ficha) en la que está dentro de la consola. Cuando se accede a la ayuda contextual, se abre la guía del usuario para el producto asociado con la ubicación en una nueva ventana y muestra el tema correspondiente.

La biblioteca de documentación es una página dentro de Symantec Management Console que permite acceder a la documentación que se proporciona con cada producto instalado, como guías del usuario, guías de administración, guías de implementación y notas de la versión. La documentación se encuentra en el equipo con Notification Server, como las guías del usuario, o en un sitio web, como las notas de la versión. Parte de la documentación está en formato de Adobe Acrobat y necesita Adobe Acrobat Reader para verse o para imprimirse.

Ver "Acerca de Symantec Management Console" en la página 34.

Para acceder a la documentación de la ayuda contextual

1. En Symantec Management Console, asegúrese de que la ubicación en la que desee acceder a la ayuda esté activa.

   Para activar una ubicación, haga clic en alguna parte en la ubicación. Por ejemplo, haga clic en la página o el cuadro de diálogo.

2. Efectúe uno de los pasos siguientes:

   - En el menú **Ayuda**, haga clic en **Contexto**.
   - Presione la tecla **F1**.

Para acceder a la biblioteca de documentación

1. En Symantec Management Console, en el menú **Ayuda**, haga clic en **Biblioteca de documentación**.
2. En la página **Biblioteca de documentación**, haga clic en el vínculo asociado con la documentación a la que desee acceder.

Acceder a la página Mi portal

La página Mi portal es la página predeterminada que aparece cuando un nuevo usuario abre Symantec Management Console.

Los cambios que un usuario realice a la página Mi portal, tales como agregar, editar o quitar elementos web, se personalizan para ese usuario. Los cambios se guardan

según su Id. de usuario. La próxima vez que el usuario inicia sesión y selecciona la opción de página Mi portal en el menú Consola, la página Mi portal personalizada se vuelve a cargar automáticamente.

Ver "Creación y modificación de páginas del portal" en la página 59.

Para acceder a la página Mi portal

- En Symantec Management Console, en el menú **Inicio**, haga clic en **Mi portal**.

Acceso a la página inicial de Administración de Notification Server

La página inicial de Administración de Notification Server proporciona acceso a información clave de Notification Server y las soluciones instaladas.

La página principal de la Administración de Notification Server incluye la siguiente información:

Administrador de recursos	Un vínculo que permite seleccionar un recurso para verlo en la consola del Administrador de recursos.
Productos instalados	La lista de soluciones que están instaladas en Notification Server.
Servidores de sitio	La lista de servicios y servidores de sitio que se incluyen en el sitio de Notification Server.
Jerarquía	Los detalles de la jerarquía a la cual Notification Server pertenece. Se visualiza esta información solamente si Notification Server es un miembro de una jerarquía.
Estado de la distribución del agente	Estado de la instalación distribuida de Symantec Management Agent en los equipos que desee administrar.
Licencias	Enumera las siguientes propiedades de cada solución: ■ El número total de licencias disponibles ■ La cantidad de licencias en uso ■ Las fechas de vencimiento de las licencias (si corresponde)

La página principal de la Administración de Notification Server, como todas las páginas del portal, es personalizable. Es posible configurar la página con la información que considere más útil.

Ver "Creación y modificación de páginas del portal" en la página 59.

Para tener acceso a la página principal de la Administración de Notification Server

- En Symantec Management Console, en el menú **Inicio**, haga clic en **Administración de Notification Server > Portal**.

Personalización de Symantec Management Console

El usuario puede personalizar Symantec Management Console para que se adapte a los requisitos de su organización. Por ejemplo, se pueden agregar elementos adicionales del submenú al menú de la consola a fin de que satisfaga las necesidades de los usuarios en su organización. No es posible cambiar las opciones superiores del menú ni editar o quitar ninguno de los elementos del submenú incluidos en Symantec Management Console.

La mayoría de los procesos de personalización se aplican a todo el sistema. Para lograr una personalización de niveles de rol, se puede usar seguridad en los elementos. Por ejemplo, se puede crear una página del portal que sea accesible solamente a cierto rol. En este caso, la personalización se aplica con permisos para los elementos, en lugar de privilegios. Además, las vistas, los árboles y los menús se pueden personalizar usando seguridad. Por ejemplo, un administrador de Symantec puede establecer el permiso en una opción de elemento o de menú de árbol, de modo que los usuarios con cierto rol puedan verlo, pero no los usuarios con otro rol. Sin embargo, la página Mi portal y la personalización por página se aplica por cada usuario.

Tabla 2-4 Tareas de personalización

Tarea	Descripción
Personalice los menús	Agregue submenús y elementos del submenú, y configure la estructura del menú de forma que satisfaga las necesidades de su organización. Ver "Personalización del menú de la consola" en la página 53.
Personalice los menús contextuales	Agregue acciones definidas por el usuario al menú contextual. Ver "Adición de acciones definidas por el usuario en el menú contextual" en la página 55.

Tarea	Descripción
Personalice las vistas	Cree y modifique las vistas para configurar la estructura del árbol de navegación como mejor le convenga a su organización. Ver "Creación y modificación de vistas" en la página 57. Ver "Adición de nuevos elementos directamente en una vista" en la página 58.
Personalice las páginas del portal	Cree y modifique las páginas del portal. Una página del portal es una página de Symantec Management Console que se puede personalizar para satisfacer sus requisitos. El usuario tiene la posibilidad de usar una página del portal para consolidar la información clave en una sola página fácil de visualizar. Una página del portal permite visualizar el estado de Symantec Management Platform y de los equipos administrados, o cualquier otro tipo de información que se desee poner a disposición. Por ejemplo, se pueden incluir páginas web externas, páginas de intranet, fuentes RSS o aplicaciones propias. Ver "Creación y modificación de páginas del portal" en la página 59.
Personalice los elementos web	Cree y modifique los elementos web que utiliza para generar las páginas del portal. Ver "Creación y modificación de elementos web" en la página 61.

Es posible guardar los elementos personalizados de la consola como archivos XML y restaurarlos cuando sea necesario mediante la importación de los archivos apropiados.

Ver "Cómo guardar elementos de la consola como archivos XML" en la página 63.

Personalización del menú de la consola

El usuario tiene la posibilidad de personalizar el menú de la consola a fin de adaptarla a sus requisitos. Las opciones del menú que se proporcionan con Symantec Management Platform son de sólo lectura y no se pueden modificar. Es posible agregar nuevos submenús y modificarlos según sea necesario. Los elementos del menú se pueden mover o eliminar, excepto los señalados como de solo lectura.

Ver "Personalización de Symantec Management Console" en la página 52.

Para personalizar el menú de la consola

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Consola > Menús**.
2. En la página **Editar menú**, realice las tareas de personalización adecuadas:

Para agregar elementos del menú	1. En el panel izquierdo, haga clic con el botón derecho en el elemento de menú bajo el cual desee agregar el nuevo elemento de menú y después haga clic en **Elemento nuevo**. 2. En la página **Detalles del menú**, especifique los detalles del elemento de menú y después haga clic en **Aplicar**.
Para agregar submenús	1. En el panel izquierdo, haga clic con el botón derecho en el elemento de menú bajo el cual desee agregar el submenú y después haga clic en **Submenú nuevo**. 2. Haga clic en **Aplicar**.
Para importar elementos de submenú desde un archivo XML	1. En el panel izquierdo, haga clic con el botón derecho en el submenú al cual desee importar los elementos de menú y después haga clic en **Importar submenú**. 2. En el cuadro de diálogo **Elija el archivo XML que desea importar**, seleccione el archivo XML apropiado y después haga clic en **Abrir**. 3. Haga clic en **Aplicar**.
Para exportar un submenú a un archivo XML	1. En el panel izquierdo, haga clic con el botón derecho en el submenú que desee exportar y después haga clic en **Exportar...**. 2. En el cuadro de diálogo **Archivo de destino para XML exportado**, especifique el nombre y la ubicación del archivo XML, y después haga clic en **Guardar**.

Para importar todo el menú de la consola de un archivo XML	1 En el panel izquierdo, en la barra de herramientas, haga clic en el icono **Importar todo el menú**. 2 En el cuadro de diálogo **Elija el archivo XML que desea importar**, seleccione el archivo XML apropiado y después haga clic en **Abrir**.

Adición de acciones definidas por el usuario en el menú contextual

El menú contextual de la consola (al que se accede haciendo clic con el botón derecho) contiene las opciones del menú que son relevantes para la carpeta o el elemento donde se hizo clic. Con Notification Server se proporciona un conjunto predeterminado de opciones de menú contextual, y las soluciones instaladas pueden agregar otras opciones. La mayor parte del conjunto de opciones predeterminadas son funciones comunes que están disponibles en la mayoría de las carpetas y los elementos.

Es posible crear acciones definidas por el usuario y hacer que estén disponibles en el menú contextual. Efectúe una de las siguientes acciones:

- Abra una URL y sustituya los detalles del recurso seleccionado en la URL. Por ejemplo, el nombre del recurso.
- Ejecute una línea de comandos en el equipo con Notification Server o el equipo en el cual el explorador está en ejecución.

Nota: Cada usuario que desee ejecutar las acciones con el botón derecho de la línea de comandos necesita tener el certificado SSL apropiado instalado en el equipo. Es posible descargar el certificado SSL que se necesita de la página **Certificado de acción con el botón derecho de línea de comandos**.

Para especificar los recursos a los que se aplica la acción, seleccione el tipo de recurso y filtre (opcional) los recursos con una consulta. Cuando haga clic con el botón derecho en un recurso del tipo apropiado que cumple la consulta del filtro (si se especificó un filtro), el menú contextual que aparece incluye la acción definida por el usuario.

Se necesita el privilegio de Nueva Acción con el botón secundario del ratón para poder agregar una acción definida por el usuario al menú contextual.

Ver "Categorías de privilegios de seguridad" en la página 489.

Para agregar una acción definida por el usuario al menú contextual

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Consola > Acciones con el botón secundario del ratón**.
2. En el panel izquierdo, haga clic con el botón derecho en la carpeta a la que desea agregar Acción con el botón secundario del ratón y, a continuación, haga clic en **Nueva > Acción con el botón secundario del ratón**.
3. En la página **Nueva acción de clic con botón secundario**, especifique el nombre y la descripción apropiados.
4. Configure la acción que desee con la configuración apropiada:

Activar	La acción se debe habilitar para ser incluida en el menú contextual. La nueva acción se deshabilita de forma predeterminada, lo que permite configurar y probar la acción antes de que esté disponible para usuarios de la consola.
Tipo de recurso	El tipo de recurso al que se aplica la acción. De forma predeterminada, todos los recursos del tipo especificado están incluidos. Si desea aplicar la acción a un subconjunto específico de recursos, puede filtrar los recursos con una expresión de consulta adecuada.
Tipo de acción	En la lista desplegable, seleccione el tipo de acción apropiado: ■ URL En el cuadro URL básica, especifique la dirección URL apropiada. La dirección URL puede dirigirlo a otra página en Symantec Management Console, a una intranet o a un sitio de Internet externo. ■ Línea de comandos En el cuadro **Línea de comandos**, especifique la línea de comandos apropiada. Compruebe la casilla **Ejecutar en el servidor** para ejecutar la línea de comandos del servidor. Si deja esta casilla con la selección anulada, la línea de comandos se ejecuta en el equipo desde el que se invoca la acción.

Parámetros de sustitución	Los parámetros de sustitución permiten usar una variable en la línea de comandos o en la dirección URL y tener el valor sustituido con el valor apropiado en el tiempo de ejecución. Por ejemplo, el nombre del recurso, la dirección IP o el GUID. Para cada parámetro de sustitución que desee incluir: 1 Haga clic en **Agregar**. 2 En la ventana **Seleccionar atributos**, seleccione el atributo que desee usar como parámetro y, a continuación, haga clic en **Aceptar**. 3 En **Nombre del parámetro**, escriba el nombre apropiado para el parámetro.

5 Haga clic en **Aplicar**.

Ver "Personalización de Symantec Management Console" en la página 52.

Creación y modificación de vistas

Notification Server y las soluciones incluyen vistas predefinidas que se pueden modificar y ampliar según sea necesario. También se pueden crear y modificar sus propias vistas.

Ver "Acerca de las vistas de la consola" en la página 36.

Para crear o modificar una vista

1 En Symantec Management Console, en el menú **Configuración**, haga clic en **Consola > Vistas**.

2 En el panel izquierdo, en la carpeta **Vistas**, realice una de las siguientes acciones:

Para crear una nueva vista	Haga clic con el botón derecho en la carpeta en la cual desea agregar la vista y, luego, seleccione **Nueva > Vista**.
Para modificar una vista existente	Haga clic con el botón derecho en la vista que desea modificar y, a continuación, seleccione **Editar vista**.

3 En la página **Editar vista**, especifique los detalles adecuados en los siguientes campos:

Nombre	Nombre de la vista.

Descripción	Descripción de la vista.
Mostrar página del portal	Le permite seleccionar una página del portal para asociar con la carpeta raíz de la vista. Cuando la carpeta raíz de la vista está seleccionada en el panel izquierdo, la página del portal que se haya especificado se visualiza en el contenido del panel.
Contenido de esta vista	Visualiza la estructura de la vista que está creando y permite crear nuevas carpetas y eliminar los elementos que no desea. El contenido se ordena alfabéticamente, con las carpetas en la parte superior y, a continuación, los elementos. No es posible modificar la estructura.
Elementos disponibles	Muestra la estructura de árbol de Symantec Management Console y permite seleccionar las carpetas y los elementos que desea incluir en la vista. Para agregar un elemento a la vista 1 En la lista desplegable **Árbol**, seleccione el árbol del cual desee seleccionar elementos. 2 Expanda el árbol y seleccione la carpeta o el elemento que desea agregar a la vista. 3 Haga clic en **Agregar**.

4 Haga clic en **Aceptar**.

Adición de nuevos elementos directamente en una vista

Se pueden agregar nuevas carpetas, vínculos de elementos y vínculos web directamente en una vista. También se pueden agregar nuevas vistas para crear una jerarquía.

Ver "Acerca de las vistas de la consola" en la página 36.

Para agregar un nuevo componente directamente en una vista

1 En Symantec Management Console, en el menú **Configuración**, haga clic en **Consola > Vistas**.

2 En el panel izquierdo, haga clic con el botón derecho en la carpeta en la cual desee agregar la nueva carpeta o elemento, y seleccione la opción correspondiente:

Nuevo > Carpeta	En el cuadro de diálogo **Nueva carpeta**, escriba el nombre de la nueva carpeta y después haga clic en **Aplicar**.
Nuevo > Vínculo del elemento	En la ventana **Editar el vínculo del elemento**, seleccione el elemento para el cual desee crear un vínculo y haga clic en **Aceptar**.
Nuevo > Vínculo web	En el cuadro de diálogo **Configuración del vínculo web**, especifique la URL de la página web con la cual desee establecer el vínculo. De forma opcional, es posible especificar lo siguiente: ■ URL de la imagen del icono Si desea usar un icono en la vista de árbol, especifique la URL que apunta al archivo de imagen correspondiente. ■ Marco de destino La opción predeterminada es el panel derecho, que es el área principal de contenido generalmente conocida como panel derecho. Haga clic en **Aplicar**.
Nuevo > Vista	En la ventana **Editar vista**, cree la vista deseada. Ver "Creación y modificación de vistas" en la página 57.

Creación y modificación de páginas del portal

Una página del portal es una página de Symantec Management Console que se puede personalizar para satisfacer sus requisitos. El usuario tiene la posibilidad de usar una página del portal para consolidar la información clave en una sola página fácil de visualizar. Una página del portal permite mostrar el estado de Symantec Management Platform y de los equipos administrados, o cualquier otro tipo de información que se desee poner a disposición. Por ejemplo, se pueden incluir páginas web externas, páginas de intranet, fuentes RSS o aplicaciones propias. Esto es más conveniente que visualizar varias páginas de consola para recopilar la información deseada.

Ver "Personalización de Symantec Management Console" en la página 52.

La mayoría de las páginas del portal están disponibles para todos los usuarios de la consola. La excepción es la página Mi portal, que es una página del portal especial, única para cada usuario.

Ver " Acceder a la página Mi portal" en la página 50.

Nota: Para ver una página del portal, se requiere permiso de lectura de esa página del portal.

Las páginas del portal se construyen a partir de elementos web. Es posible crear y personalizar elementos web según sus requisitos y después agregarlos a las páginas del portal.

Los tipos de elementos web son los siguientes:

Informe	Muestra la información que se recupera de un informe.
URL	Un vínculo a otra página web (por ejemplo, una página de la intranet corporativa o un sitio web externo).

Las páginas del portal pueden tener hasta tres columnas. Los elementos web se pueden ver en una página del portal en tres tamaños diferentes, según en qué columna se encuentren o si ocupan todas las columnas. La columna izquierda y la del medio tienen el mismo ancho (los elementos web que aparecen en ellas son “pequeños”) y la columna derecha es más ancha (sus elementos web son “grandes”). Como alternativa, un elemento web puede usar todo el ancho de la página (el elemento web es “de varias columnas”). Estos elementos web de varias columnas pueden verse en la parte superior o inferior de la página del portal. Cuando se diseña un elemento web nuevo, es necesario asegurarse de que se visualice apropiadamente en cualquier tamaño. No es posible establecer un tamaño determinado como propiedad del elemento web.

Es posible contraer un elemento web haciendo clic en la flecha que se encuentra en la parte superior derecha y expandirlo volviendo a hacer clic en la flecha. Esto permite incluir elementos que se cargan con lentitud o que se usan con poca frecuencia en una página del portal.

Las páginas del portal tienen los dos modos de operación siguientes:

Ver	La página del portal es de sólo lectura. Es posible ver todos los elementos web, pero no se puede realizar ningún cambio. Algunas páginas del portal proporcionadas por las soluciones de Symantec pueden estar restringidas al modo de vista para impedir que cualquier persona modifique el contenido.
Editar	Si tiene permiso de escritura en la página del portal, significa que puede editarla. El usuario puede agregar, quitar, redimensionar y reordenar los elementos web en una página del portal. El árbol de los elementos web se visualiza en el sector izquierdo de la página, lo que permite arrastrar los elementos web y soltarlos en las ubicaciones adecuadas. Para quitar un elemento web de una página del portal, haga clic en el símbolo X que se encuentra en la esquina superior derecha del elemento web.

Ver "Creación y modificación de elementos web" en la página 61.

Para crear o modificar una página del portal

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Consola > Páginas del portal**.
2. Efectúe uno de los pasos siguientes:

Para crear una nueva página del portal	En el panel izquierdo, haga clic con el botón derecho en la carpeta **Páginas del portal** y, a continuación, seleccione **Nuevo > Página del portal**.
Para modificar una página del portal existente	En el panel izquierdo, en la carpeta **Páginas del portal**, seleccione la página que desee editar. En la esquina superior derecha de la página del portal, haga clic en **Editar**.

3. En la página **Configuración de la página del portal**, especifique el nombre y la descripción de la página, y seleccione los elementos web que desee usar en la página del portal.

Nombre	El nombre de la página del portal.
Descripción	Una descripción de la página del portal.
Panel Elementos web	Este panel contiene la lista de elementos web disponibles que se pueden agregar a la página del portal. Para agregar un elemento web: 1 Seleccione el elemento web y después haga clic en **Agregar**. 2 En la página del portal, haga clic en el elemento web y arrástrelo a la ubicación adecuada de la página.

4. Si desea quitar un elemento web de la página, en el marco Elemento web adecuado, haga clic en el símbolo **Eliminar** ubicado en la esquina superior derecha.
5. Haga clic en **Aplicar**.

Creación y modificación de elementos web

Los elementos web son las minipáginas web que se pueden usar como bloques de creación para páginas del portal. Un elemento web puede visualizar un informe

o el contenido de una página web. La consola se suministra con un conjunto de elementos web predefinidos, que se pueden usar para crear las páginas del portal. Es posible modificar estos elementos web y, además, crear nuevos.

Ver "Creación y modificación de páginas del portal" en la página 59.

También se puede crear un elemento web de informe directamente a partir de un informe.

Ver "Cómo guardar los resultados del informe de Notification Server como un elemento web" en la página 448.

Para crear o modificar un elemento web

1 En Symantec Management Console, en el menú **Configuración**, haga clic en **Consola > Elementos web**.

2 Efectúe uno de los pasos siguientes:

Para crear un nuevo elemento web	En el panel izquierdo, expanda la carpeta **Elementos web** y haga clic con el botón derecho en la carpeta en la cual desea agregar el nuevo elemento web. Haga clic en **Nuevo > Elemento web**.
Para modificar un elemento web existente	En el panel izquierdo, expanda la carpeta Elementos web y seleccione el elemento web que desee modificar.

3 En la página **Configuración de elemento web**, especifique los parámetros de los elementos web:

Nombre	El nombre del elemento web.
Descripción	Una descripción del elemento web.
Contenido de elemento web	El contenido del elemento web. Es posible elegir una de las siguientes opciones: ■ Resultados del informe Si elige esta opción, debe seleccionar el informe apropiado. El informe se ejecuta cuando se abre una página del portal que contiene el elemento web, de forma que los resultados siempre están actualizados. ■ Mostrar URL Si elige esta opción, especifique la dirección URL adecuada.

Altura fija	Seleccione esta opción para especificar una altura fija para el elemento web y, luego, escriba la altura (en píxeles) en el cuadro adyacente. Si no se selecciona esta opción, el tamaño del elemento web cambia según el contenido que muestra.
Tamaño predeterminado	El tamaño predeterminado del elemento web: ■ Pequeño ■ Grande ■ Varias columnas Cuando se agrega el elemento web a una página del portal, su ubicación predeterminada se determina según su tamaño predeterminado. Si mueve el elemento web a otra ubicación, su tamaño cambia automáticamente.

4 Si desea cancelar los cambios sin guardar, haga clic en **Cancelar**.

5 Haga clic en **Guardar cambios**.

6 Si desea obtener una vista previa del elemento web especificado, haga clic en **Mostrar vista previa**.

Cómo guardar elementos de la consola como archivos XML

Es posible guardar los elementos de la consola (elementos del menú, vistas, páginas del portal o elementos web) como archivos XML. Es conveniente hacer esto para crear archivos de copia de seguridad antes de personalizar la consola. También sirve para crear archivos XML, que se pueden personalizar e importar como elementos de la consola personalizados en otro equipo Notification Server.

Ver "Personalización de Symantec Management Console" en la página 52.

Para restaurar elementos de la consola, se los debe importar desde los archivos XML apropiados. Los elementos de la consola se identifican por los GUID. Los elementos del archivo XML importado sobrescriben los elementos existentes cuyo GUID coincide. Cualquier elemento de los XML cuyo GUID no coincida en la consola se agrega como elemento nuevo.

Nota: Se necesita el privilegio de importar archivos XML para poder importarlos. De forma predeterminada, solamente el rol de administrador de Symantec tiene este privilegio.

Para guardar un elemento de la consola como archivo XML

1. En Symantec Management Console, en el panel izquierdo, haga clic en el nodo del árbol que desea guardar.
2. Haga clic con el botón derecho y, a continuación, haga clic en **Exportar**.
3. En el cuadro de diálogo **Archivo de destino para XML exportado**, especifique el nombre y la ubicación del archivo XML, y después haga clic en **Guardar**.

Para restaurar un elemento de la consola desde un archivo XML

1. En Symantec Management Console, en el panel izquierdo, seleccione la carpeta en la cual desea restaurar el elemento.
2. Haga clic con el botón derecho y, a continuación, haga clic en **Importar**.
3. En el cuadro de diálogo **Elija el archivo XML que desea importar**, seleccione el archivo XML adecuado.
4. Si desea evitar que se realice cualquier cambio al elemento importado, seleccione **Abrir sólo lectura**.
5. Haga clic en **Abrir**.

Sección 2

Cómo configurar los servidores de Symantec Management Platform

- Capítulo 3. Cómo configurar Notification Server
- Capítulo 4. Configuración de seguridad
- Capítulo 5. Configuración de programaciones
- Capítulo 6. Configurar los sitios y los servidores de sitio
- Capítulo 7. Configuración de Package Server para Linux
- Capítulo 8. Configuración de la jerarquía
- Capítulo 9. Configuración de la replicación
- Capítulo 10. Cómo realizar una configuración por primera vez

Capítulo 3

Cómo configurar Notification Server

En este capítulo se incluyen los temas siguientes:

- Acerca de Notification Server
- Acerca de configurar Notification Server
- Cómo configurar los valores de Notification Server
- Cómo configurar los valores de Notification Server con el configurador de NS
- Cómo configurar la base de datos de administración de configuración
- Depuración de base de datos de administración de configuración
- Almacenamiento del historial de datos de recursos en la CMDB

Acerca de Notification Server

Notification Server es el componente del servidor principal de Symantec Management Platform. Notification Server coordina las diversas soluciones y proporciona la interfaz de usuario principal, la administración basada en políticas, la elaboración de informes y la notificación. Notification Server alberga la consola de administración basada en Web que le permite administrar los componentes de su Symantec Management Platform.

Ver "Componentes de Symantec Management Platform" en la página 28.

Ver "Acerca de configurar Notification Server" en la página 67.

Notification Server es responsable de administrar las políticas y las tareas predefinidas que están disponibles en cada solución instalada. Estas políticas y

tareas activan los componentes de Notification Server que procesan varias funciones.

Las funciones de Notification Server incluyen lo siguiente:

- Cómo detectar recursos en la red
- Instalación y configuración del agente de administración en los endpoints
- Recopilación de la información de los clientes y almacenamiento en la CMDB
- Generación de informes web detallados
- Envío de información de políticas a los endpoints
- Distribución de paquetes de software

Acerca de configurar Notification Server

La configuración predeterminada de Notification Server es conveniente para la mayoría de los propósitos y, normalmente, no necesita cambiarla. Se especifica esta configuración predeterminada cuando se instala Symantec Management Platform. Sin embargo, como las necesidades de la organización cambian, se pueden realizar los cambios de configuración apropiados.

Ver "Acerca de Notification Server" en la página 66.

Tabla 3-1 Tipos de configuración

Configuración	Descripción
Establezca la configuración de la Base de datos de la administración de configuración (CMDB).	Ver "Cómo configurar la base de datos de administración de configuración" en la página 76.
Configure la depuración de la base de datos.	Ver "Depuración de base de datos de administración de configuración" en la página 80.
Configure la retención del historial de datos del recurso.	Ver "Almacenamiento del historial de datos de recursos en la CMDB" en la página 82.
Configure los valores de Notification Server. Esta configuración incluye procesamiento de eventos, registro de mensajes de estado, servidor de mensajes de correo electrónico y direcciones predeterminadas, y un servidor proxy.	Ver "Cómo configurar los valores de Notification Server" en la página 68.

Configuración	Descripción
Configure los valores de Notification Server que no aparecen en Symantec Management Console.	Ver "Cómo configurar los valores de Notification Server con el configurador de NS" en la página 75.
Especifique las credenciales del punto de distribución de paquetes de Software Delivery.	Ver "Configuración de las credenciales del punto de distribución" en la página 75.

Cómo configurar los valores de Notification Server

Las opciones de Notification Server que puede configurar incluyen el procesamiento de eventos, el registro de mensajes de estado y las direcciones predeterminadas y el servidor de mensajes de correo electrónico.

Ver "Acerca de configurar Notification Server" en la página 67.

Es posible también configurar los otros valores de Notification Server con el configurador de NS.

Ver "Cómo configurar los valores de Notification Server con el configurador de NS" en la página 75.

Para configurar las opciones de Notification Server.

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Todas las configuraciones**.
2. En el panel izquierdo, en la carpeta **Configuración**, expanda **Notification Server** y después haga clic en **Valores de configuración de Notification Server**.

3 En la página **Valores de configuración de Notification Server**, realice los cambios apropiados en las fichas siguientes:

Procesamiento	Puede habilitar o deshabilitar un procesamiento de eventos de Notification Server (NSE), especificar la identidad de aplicación de Notification Server y reiniciar de forma manual los servicios de Notification Server. Ver "Configuración de procesamiento de Notification Server" en la página 69.
Correo electrónico	Puede especificar el servidor de correo electrónico que Notification Server utiliza y establecer las direcciones de correo electrónico predeterminadas para los campos De y Para. Ver "Configuración del servidor de correo y las direcciones" en la página 72.
Registro	Puede especificar los tipos de mensajes de estado, como advertencias, mensajes de información y errores de Notification Server, que desea registrar en Notification Server. Ver "Configuración del registro de mensajes de estado" en la página 72.
Proxy	Si no desea permitir que los usuarios de Notification Server tengan acceso directo a la red, puede configurar un servidor proxy. Ver "Configuración del servidor proxy" en la página 74.
Credenciales del punto de distribución	Puede especificar las credenciales que utiliza Notification Server para acceder a sus puntos de distribución de paquete. Ver "Configuración de las credenciales del punto de distribución" en la página 75.

4 Haga clic en **Aceptar**.

Configuración de procesamiento de Notification Server

En la ficha **Procesamiento**, se puede habilitar o deshabilitar el procesamiento de un evento de Notification Server (NSE) y especificar la identidad de la aplicación Notification Server. Un NSE es un archivo XML que se pasa entre Notification Server y Symantec Management Agent (incluidos los complementos de la solución).

En esta ficha, se puede también configurar la comunicación de agente de una versión anterior.

Ver "Cómo configurar los valores de Notification Server" en la página 68.

Tabla 3-2 Opciones en la ficha **Procesamiento**

Opción	Descripción
Procesamiento de servidor	Procesamiento de servidor se encuentra habilitado de forma predeterminada cuando instala Notification Server, pero puede haber ocasiones cuando necesite deshabilitarlo o volver a habilitarlo. Por ejemplo, cuando instala una solución, se detienen automáticamente todos los procesamientos de eventos. Después de finalizar la instalación, el procesamiento de eventos se deberá reiniciar automáticamente. Si esto no sucede, aparecerá un mensaje de advertencia en Symantec Management Console y se le solicitará que vuelva a habilitar el evento de Notification Server (NSE) de forma manual. Para volver a habilitar el procesamiento de NSE, haga clic en el mensaje de advertencia y luego, en el cuadro de diálogo que aparece, haga clic en **Reanudar**. Los NSE que se reciben mientras el proceso de NSE está deshabilitado se almacenan en el equipo con Notification Server y se administran una vez que el proceso de NSE se habilita de nuevo. Los NSE contienen información tal como la siguiente: ■ Comunicación con Symantec Management Agent ■ Procesamiento de eventos ■ Inventario básico o inventario completo ■ Éxito o error en la descarga del paquete

Opción	Descripción
Identidad de aplicación	La identidad de aplicación de Notification Server es la cuenta bajo la que ejecuta el Notification Server. Puede especificar el nombre de usuario y contraseña apropiados cuando instala Notification Server, y solo necesitará actualizar cuando sea necesario. Por ejemplo, si su organización tiene una política de cambio de contraseña, las credenciales de acceso a la CMDB quizá deban cambiarse. La identidad de aplicación no tiene más permisos para iniciar sesión en SQL Server. **Advertencia:** No puede utilizar caracteres especiales en el nombre de usuario o contraseña de la identidad de aplicación. Solo puede utilizar caracteres alfanuméricos. El Id. del usuario que define requiere los siguientes permisos: ■ Los permisos del administrador local en Notification Server y los equipos remotos con Windows 2000/XP/2003/Vista donde desea instalar Symantec Management Agent. ■ Permiso para actuar como parte del sistema operativo e iniciar sesión como trabajo en lotes y un servicio. ■ Permiso para iniciar sesión en SQL Server. Si el Id. del usuario no tiene este permiso, puede especificar un nombre de usuario y contraseña diferentes para iniciar sesión en la CMDB. ■ Permiso para conectar al SQL Server al que se puede adjuntar Notification Server. Por ejemplo, una base de datos de SMS para Web Administrator para SMS o una base de datos de concesiones para Contract Management Solution. Los servicios de Notification Server se vuelven a iniciar de forma automática cuando cambia una identidad de aplicación. Sin embargo, la opción **Reiniciar los servicios** permite reiniciar de forma manual los servicios cuando sea necesario. Por ejemplo, si desea realizar un cambio a la base de datos, se deberán reiniciar los servicios para que los cambios cobren efecto. Si la contraseña de identidad de aplicación no es correcta, Notification Server no podrá acceder a la CMDB. No puede restablecer la identidad mediante Symantec Management Console, ya que la consola utiliza la misma contraseña para acceder al Notification Server. Deberá utilizar la utilidad de ASConfig para acceder directamente a los servicios web y restablecer la contraseña de la identidad de aplicación mediante el uso de la línea de comandos apropiada.

Opción	Descripción
Comunicación de agente de una versión anterior	Le permite controlar si los endpoints que usan versiones anteriores de Symantec Management Agent pueden comunicarse con el Notification Server actualizado. Si se desactiva el modo **Comunicación de agente de una versión anterior** (LAC), se puede administrar activamente solo los agentes actualizados. Si se activa el modo LAC, se puede realizar un conjunto limitado de funciones de administración en los agentes de versiones anteriores. Ver "Acerca de la comunicación de agente de una versión anterior" en la página 272.

Configuración del servidor de correo y las direcciones

Puede definir un servidor de correo y las direcciones de los campos De y Para en los mensajes de correo electrónico de Notification Server. Notification Server utiliza SMTP para enviar mensajes de correo electrónico. La dirección de correo electrónico puede ser cualquier dirección de SMTP válida que reconozca el servidor SMTP.

Ver "Cómo configurar los valores de Notification Server" en la página 68.

Puede habilitar las soluciones de Symantec para que envíe mensajes de correo electrónico basados en los datos que recibe Notification Server. La dirección de correo electrónico que especifica podrá recibir avisos de informes que se ejecutaron con éxito, acciones automatizadas que se desarrollaron y comprobaciones de escalabilidad del sistema. Estos mensajes de correo electrónico lo ayudan a supervisar y administrar las actividades de Notification Server.

La configuración de correo electrónico se establece cuando instala Notification Server y generalmente no se necesita cambiarla. Sin embargo, si cambia el servidor SMTP o si desea que alguien más reciba los mensajes de correo electrónico, deberá realizar los cambios apropiados.

La opción **Enviar correo electrónico de prueba** permite probar la configuración de dirección y servidor de correo electrónico al enviar un mensaje con la configuración actual. Necesitará confirmar los cambios al hacer clic en Aceptar antes de enviar el correo electrónico de prueba.

Configuración del registro de mensajes de estado

Puede especificar los tipos de mensajes de estado, como advertencias, mensajes de información y errores de Notification Server, que desea registrar en Notification Server. De forma predeterminada, los mensajes de registro que Notification Server

genera se escriben en archivos de registro en el directorio `...\Program Files\Altiris\Notification Server\Logs`.

Nota: Cuando actualiza Notification Server de la versión 6.x a la7.x, el asistente de migración escribe cualquier mensaje en la ubicación del archivo de registro 6.x en lugar de la ubicación del archivo de registro 7.0. La ubicación del archivo de registro 6.x es `...\Program Files\Altiris\Notification Server\Logs`. Es necesario mirar este archivo de registro para ver los errores en la migración. El Visor de registros muestra solamente los registros que se archivan en la ubicación predeterminada 7.0. Las entradas de registro de migración no están incluidas.

Ver "Cómo configurar los valores de Notification Server" en la página 68.

Puede registrar cualquiera de los siguientes tipos de mensaje:

- Errores
- Advertencias
- Información
- Rastreo
- Detallado

También puede seleccionar almacenar archivos de registro que superen un tiempo determinado. Si configura esta opción, los archivos de registro relevantes se archivarán todos los días a las 5:00 a. m.

Ver "Abrir el visor de registros" en la página 73.

Abrir el visor de registros

El visor de registros le permite supervisar varias ubicaciones de registros para diversos componentes como IT Management Suite, Symantec Management Agent y Symantec Installation Manager. El visor de registros detecta de forma automática si el componente está instalado en una ubicación personalizada y supervisa la ruta personalizada. El visor de registros enumera en tiempo real los eventos, los errores y las advertencias que ocurren al realizar cualquier acción. Estos mensajes lo ayudan a supervisar y solucionar problemas en Notification Server.

Es posible usar el visor de registros para determinar los problemas y su causa. Una vez que se identifican los errores o las advertencias en el visor de registros, puede usar los mensajes de error para buscar artículos que podrían ayudarlo a corregir el error en la Base de conocimientos de Symantec. Es posible también plantear la cuestión al equipo de soporte técnico.

El visor de registros le permite realizar las siguientes tareas:

- Ver mensajes detallados y mensajes de seguimiento, información, advertencia y error.
- Buscar en los registros y ver los resultados.
- Marcar los elementos del registro.
- Filtrar los registros para mostrar un subconjunto de mensajes.
- Guardar las definiciones de filtros para su uso posterior.
- Realizar una búsqueda en los archivos de registro sin cargarlos en el visor de registros.

Ver "Configuración del registro de mensajes de estado" en la página 72.

La versión 7.5 de IT Management Suite introduce un nuevo visor de registros con mejores funcionalidades y una mejor capacidad de uso. Tenga en cuenta que también puede usar el visor de registros de Altiris anterior, que permanece en el producto por cuestiones de compatibilidad, ahora llamado Visor de registro de Altiris de versión anterior.

Para abrir el nuevo visor de registros

- En el equipo con Notification Server, haga clic en **Inicio** y después haga clic en **Todos los programas > Symantec > Diagnóstico > Altiris Log Viewer**.

Para abrir el visor de registros anterior

- En el equipo con Notification Server, haga clic en **Inicio** y después haga clic en **Todos los programas > Symantec > Diagnóstico > Herramientas anteriores > Altiris Legacy Log Viewer**.

Configuración del servidor proxy

Si no desea que los usuarios de Notification Server tengan acceso directo a la red, puede configurar un servidor proxy. Por ejemplo, si tiene Notification Server y los equipos administrados dentro del firewall de la organización, un servidor proxy proporciona seguridad. Es posible configurar un servidor proxy para proporcionar una manera segura mediante el firewall sin exponer Notification Server. Esta configuración ayuda a que Notification Server obtenga de manera segura los parches o las soluciones de descarga de sitios web externos.

Ver "Cómo configurar los valores de Notification Server" en la página 68.

Si usa un servidor proxy, puede mejorar el rendimiento de Notification Server utilizando menos ancho de banda y filtrando las solicitudes al solicitar archivos desde Internet. Un ejemplo es datos de PMImport.

La opción **Probar configuración** valida la configuración del servidor proxy al intentar conectarse con un sitio web externo.

Si los mensajes de error aparecen cuando prueba la configuración, asegúrese de que las credenciales de autentificación sean correctas. Asegúrese de que el servidor proxy esté en ejecución y que no existan errores de red generales.

Configuración de las credenciales del punto de distribución

Puede especificar las credenciales del punto de distribución (DPC) que utiliza Notification Server para acceder a sus paquetes de distribución de software. Estos paquetes se ubican en un recurso compartido de red al que se puede acceder mediante una ruta UNC. El Notification Server publica estos paquetes a un directorio HTTP virtual que utiliza el DPC para conectarse con el recurso compartido UNC.

Ver "Cómo configurar los valores de Notification Server" en la página 68.

Puede especificar las credenciales del punto de distribución antes de crear un paquete de software al que se puede acceder desde una ruta UNC existente. Las credenciales deben tener permiso para validar las cuentas de usuario y tener permiso de lectura en todos los archivos de los puntos de distribución remotos.

Notification Server puede utilizar alguna de las siguientes credenciales:

Credenciales de conectividad del agente	Todos los Symantec Management Agents utilizan las Credenciales de conectividad del agente (ACC) para conectarse a un recurso seguro. La ACC se establece en la política de Configuración global de agente.
Credenciales especificadas por el usuario	Si los paquetes se almacenan en una ubicación a la que no se puede acceder con Credenciales de conectividad del agente, puede lograr que se pueda acceder a ellos. Para poder acceder a los paquetes, especifique el nombre de usuario y la contraseña de una cuenta que cuente con acceso apropiado. No incluya caracteres especiales en el nombre o la contraseña de usuario. Solo puede utilizar caracteres alfanuméricos.

Cómo configurar los valores de Notification Server con el configurador de NS

El configurador de NS es una herramienta de configuración que permite cambiar la mayoría de los valores de configuración principales de Notification Server. Esta configuración incluye muchos valores a los que no se puede acceder desde Symantec Management Console. Es necesario usar solamente el configurador de NS para cambiar esta configuración si sabe el efecto que tiene en el sistema.

Ver "Acerca de configurar Notification Server" en la página 67.

Cuando un usuario inicia el configurador de NS, se realiza una comprobación de seguridad para determinar si el usuario tiene permiso para ver o modificar la configuración de Notification Server. Si un usuario no tiene permiso, aparece un mensaje de advertencia y se cierra la herramienta.

Para configurar los valores de Notification Server con el configurador de NS

1. Para iniciar el configurador de NS, ejecute el archivo NSConfigurator.exe.

   Este archivo está en Archivos de programa\Altiris\Notification Server\Bin\Tools. Cuando ejecuta esta herramienta, se abre el archivo CoreSettings.config que se encuentra en Archivos de programa\Altiris\Notification Server\Config.

2. Realice una de las siguientes acciones para encontrar el valor de configuración que desea cambiar:

   - En el árbol de navegación, en el panel izquierdo, localice la configuración.
   - En el campo de búsqueda, en la esquina derecha superior, especifique el texto de búsqueda y haga clic en **Buscar**. En la lista de resultados de búsqueda, haga clic en el vínculo **Mostrar** para esa configuración.

3. En el panel derecho, cambie la configuración y haga clic en **Guardar**.

   Si especifica un valor no válido para una configuración, aparece un mensaje de error. Solo es posible guardar los cambios si especifica un valor válido.

4. Para restaurar el valor predeterminado, haga clic en **Restaurar valor predeterminado**.

   La opción **Restaurar valor predeterminado** aparece solamente si la configuración tenía un valor predeterminado.

Cómo configurar la base de datos de administración de configuración

Notification Server tiene una base de datos denominada Base de datos de la administración de configuración (CMDB). Notification Server y las soluciones utilizan la CMDB para almacenar elementos de configuración y datos de recursos.

El procesamiento de la base de datos es uno de los procesos que consumen más recursos en Symantec Management Platform. El número de soluciones que están instaladas en su entorno y cómo son usadas influyen en los requisitos de la base de datos. El número de equipos administrados que se informan a cada equipo con Notification Server también influye en los requisitos de la base de datos.

Cada equipo con Notification Server se puede configurar para usar una Base de datos de administración de configuración (CMDB) local o para usar CMDB remoto. Un equipo con Notification Server con una base de datos local necesita más recursos que un equipo con Notification Server con una configuración de base de datos remota.

Es posible usar la configuración siguiente para CMDB:

Configuración de CMDB local	En una configuración de servidor de CMDB local se instala CMDB en el mismo equipo que Notification Server. Esta configuración se acepta en entornos con entre 1000 y 5000 endpoints. En estos entornos, hay contención mínima de recursos entre los servicios de Notification Server y los servicios de CMDB.
Configuración de CMDB remota	En una configuración de CMDB remota, se instala CMDB en otro equipo que no sea el equipo con Notification Server. Esta configuración se recomienda para la mayoría de los entornos. En esta configuración, la carga de trabajo de CMDB se descarga del equipo con Notification Server. El servidor de CMDB y el equipo con Notification Server deben tener una conexión de red de alta velocidad entre ellos. Symantec recomienda Ethernet de 1 GB.

Es posible realizar cualquier cambio necesario a la configuración de CMDB. Cuando Notification Server está instalado, la CMDB se configura como parte del proceso de instalación. Normalmente no es necesario hacer más cambios.

Sin embargo, puede haber ocasiones cuando es necesario cambiar la configuración de la CMDB. Por ejemplo, si se actualiza el hardware en el cual se ejecuta Microsoft SQL Server o si el Soporte de Symantec lo indica.

Para configurar la Base de datos de la administración de configuración

1 En Symantec Management Console, en el menú **Configuración**, haga clic en **Notification Server > Configuración de la base de datos**.

2 En la página **Configuración de la base de datos**, en la ficha **General** y en la ficha **Informes**, realice los cambios de configuración apropiados.

Nombre del servidor de base de datos

El nombre del SQL Server que contiene la CMDB.

Use el formato *nombredeservidor\nombredeinstancia*. Por ejemplo, **SydNS\sql_cp1_cs_as**.

Credenciales de la base de datos

El nombre de usuario y la contraseña que son necesarios para acceder a la CMDB.

Es posible usar las credenciales de la aplicación de Notification Server para la autenticación de Windows. Es posible utilizar este método para evitar ser afectado por cualquier política de cambio de contraseña que se aplique en su organización.

Las credenciales de la aplicación se especifican en la ficha **Procesamiento** de la página **Configuración del servidor**.

Ver "Configuración de procesamiento de Notification Server" en la página 69.

Además tiene la opción de usar la autenticación de SQL. Para usar la autenticación de SQL, puede especificar el nombre de usuario y la contraseña de inicio de instancia de SQL apropiados.

Nota: Si desea cambiar la autenticación de base de datos a SQL, deberá realizar este cambio en ambas fichas (**General** e **Informes**). La ficha **General** es la ficha predeterminada que aparece cuando abre la página **Configuración de la base de datos**. Si realiza el cambio solamente en la ficha **General**, Notification Server no será completamente funcional y es posible que experimente errores con algunas operaciones.

Nombre de la base de datos

Es posible seleccionar una base de datos existente de la lista de bases de datos disponibles o crear una base de datos nueva.

Si selecciona una base de datos existente, asegúrese de que sea la misma versión que Notification Server.

Reparar la base de datos

Permite reparar la CMDB. Es posible que sea necesario hacer este procedimiento cuando se restaura Notification Server desde una copia de seguridad a un nuevo equipo.

Tiempo de espera del comando	Especifique la cantidad de tiempo que Notification Server intenta procesar una consulta, como ejecutar un informe o actualizar un filtro. Es conveniente cambiar este valor por motivos de rendimiento, como una alta carga en SQL Server, lo que hace que las consultas superen el tiempo de espera. Symantec recomienda establecer el tiempo de espera del script de ASP en Microsoft IIS en un valor igual o mayor que el valor de **Tiempo de espera del comando**. Consulte al administrador de la base de datos antes de realizar cualquier cambio.
Credenciales públicas del informe	El contexto de seguridad que se usará para ejecutar las consultas de informe en la CMDB. Estas credenciales proporcionan menos seguridad que las credenciales de base de datos (que son para el administrador de la base de datos). Estas credenciales se usan para acceder a la base de datos y para ejecutar la consulta SQL apropiada cuando un usuario ejecuta un informe.

3 Haga clic en **Guardar cambios**.

Ver "Acerca de configurar Notification Server" en la página 67.

Depuración de base de datos de administración de configuración

Para administrar el tamaño de la Base de datos de administración de configuración (CMDB), puede especificar durante cuánto tiempo se almacenan ciertos tipos de datos. Es posible especificar la longitud del almacenamiento para datos como informes, equipos administrados y datos de eventos. Por ejemplo, si experimenta un bajo rendimiento al ejecutar los informes, intente depurar sus eventos o configurar las opciones de depuración para ahorrar datos.

Ver "Cómo configurar la base de datos de administración de configuración" en la página 76.

Los datos que pueden depurarse de la CMDB incluyen los siguientes:

- Instantáneas de informes
  Se eliminarán las instantáneas que son más antiguas que el tiempo especificado.
- Los equipos administrados que no se comunicaron con Notification Server durante más tiempo que el especificado

Estos pueden eliminarse o configurarse a medida que se retiran. La CMDB se actualiza cuando se ejecuta la programación de depuración de la CMDB.

- Datos de eventos de recursos
  Se eliminarán los datos de evento que son más antiguos que el tiempo especificado. Además, puede especificar una cantidad máxima de números de fila que desea retener. Si la tabla de datos de eventos alcanza este tamaño, las nuevas filas continuarán agregándose hasta la próxima actualización programada. Cuando se ejecuta el programa de depuración de CMDB, la tabla se vuelve a cortar a su tamaño máximo. La tabla se corta mediante la eliminación de las filas más viejas, incluso si los datos más viejos no se conservaron por el tiempo especificado.
  Puede utilizar las mismas opciones de configuración para todas las clases de datos, o puede establecer opciones de configuración personalizadas para todas las clases de datos. Una configuración personalizada para una clase de datos anula la configuración global. Si no se establece una configuración personalizada para una clase de datos, la configuración global se utiliza para esa clase de datos. En todos los casos se utiliza la misma programación de depuración de la CMDB.

La programación de la depuración de la CMDB es una programación de Windows que se configura al instalar Notification Server. No puede cambiarlo por la Symantec Management Console. Si desea realizar cambios, puede hacerlo mediante el Panel de control de Windows.

Para depurar la Base de datos de Administración de configuración

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Notification Server > Mantenimiento de depuración**.
2. En el panel izquierdo, en la carpeta de **Mantenimiento de depuración**, haga clic en **Mantenimiento de depuración**.

3 En la página **Mantenimiento de depuración**, establezca la configuración en las fichas siguientes:

Mantenimiento de depuración	Le permite especificar la configuración de la depuración del informe, los datos de registro del agente y la configuración de la depuración de datos del equipo. Tenga en cuenta que la opción **Depurar entradas de registro de agente obsoletas** elimina solamente los elementos con el estado **Bloqueado**. Para anular la programación de depuración y depurar el CMDB de forma inmediata, haga clic en **Depurar ahora**.
Configuración de depuración de datos de eventos de recursos	Le permite especificar la configuración de depuración de datos de eventos de recursos que desee.
Configuración de depuración de instantáneas de datos de informes	Le permite especificar la configuración de depuración de instantáneas de datos de informes. Para anular la programación de depuración y depurar el CMDB de forma inmediata, haga clic en **Depurar ahora**.

4 Haga clic en **Guardar cambios**.

Almacenamiento del historial de datos de recursos en la CMDB

Notification Server captura los datos de recursos en tiempo real a medida que recopila los datos de inventario. Puede seleccionar crear un historial de datos de recursos para cada tipo y asociación de recurso. Para cada historial, puede especificar durante cuánto tiempo desea conservar los datos de historial en la CMDB.

Ver "Cómo configurar la base de datos de administración de configuración" en la página 76.

Un historial de datos de recursos puede incluir información de cualquiera de las clases de datos. Un historial de asociación de recursos puede incluir información de cualquiera de los tipos de asociación de recursos.

Para guardar el historial de datos de recursos en la CMDB

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Notification Server > Mantenimiento de depuración**.
2. En el panel izquierdo, en la carpeta **Mantenimiento de depuración**, haga clic en **Historial de recursos**.
3. En la página **Historial de recursos** para cada tipo de asociación de recursos y tipo de clase de datos del recurso que desee configurar, es posible que desee tomar las medidas siguientes en las fichas apropiadas:
   - Amplíe la clase de datos o tipo de asociación.
   - Seleccione las clases de datos o asociaciones para las que desea crear un historial de datos de recursos.
   - Para cada asociación o clase de datos, especifique el período para el que desea el historial de datos de recursos.
     En la lista desplegable correspondiente, seleccione el período de tiempo (Días, semanas o Meses). A continuación, escriba el número apropiado de días, semanas o meses.

   Los datos de recursos más antiguos que el tiempo especificado para este tipo se eliminan de la CMDB durante la programación de depuración.
4. Haga clic en **Guardar cambios**.

Capítulo 4

Configuración de seguridad

En este capítulo se incluyen los temas siguientes:

- Acerca de la seguridad de Symantec Management Platform
- Configuración de la seguridad de Symantec Management Platform
- Tareas de administración de la seguridad de Symantec Management Platform

Acerca de la seguridad de Symantec Management Platform

Symantec Management Platform utiliza seguridad basada en roles, lo cual indica que el acceso de usuario se basa en el rol de seguridad del usuario. Un rol de seguridad es un conjunto de privilegios y permisos que se otorgan a todos los miembros de ese rol. El uso de seguridad basada en roles le permite crear y mantener un número pequeño de roles de seguridad. Es posible entonces asignar cada cuenta de usuario de Symantec Management Platform al rol apropiado, en lugar de asignar privilegios y permisos específicos a cada usuario individual. Sin embargo, se puede también asignar permisos específicos a las cuentas de usuario individuales.

Las cuentas de usuario, que a veces se denominan usuarios, no son lo mismo que recursos de usuario en Symantec Management Platform. Un recurso de usuario es una entidad que se usa para asociar los dispositivos administrados con el propietario del dispositivo. Los recursos de usuario existentes y las cuentas de usuario que pueden iniciar sesión en Symantec Management Console o ejecutar un flujo de trabajo son entidades individuales.

El rol de seguridad controla el acceso de usuario a Symantec Management Platform mediante:

- Privilegios

El privilegio es apto para todo el sistema. Los privilegios son asignados solamente a los roles y no pueden ser asignados directamente a las cuentas de usuario individuales. Un privilegio asignado a un rol permite que una cuenta de usuario que sea un miembro de ese rol realice una acción determinada en Symantec Management Platform o en Symantec Management Console. En algunos casos, el rol del usuario requiere los permisos correspondientes.
Ver "Categorías de privilegios de seguridad" en la página 489.

- Permisos en carpetas y elementos
  Los permisos especifican el acceso que tiene un rol de seguridad o una cuenta de usuario a una carpeta Symantec Management Console o un elemento. Un permiso en un rol de seguridad se aplica a todos los miembros de ese rol. Un permiso en una carpeta se aplica a todos los elementos que están contenidos directamente en esa carpeta.
  Ver "Categorías de permisos de seguridad" en la página 491.
- Permisos en vistas y grupos organizativos
  Una vista organizativa es un grupo jerárquico de recursos (como grupos organizativos) que refleja una estructura real, o vista, de su organización. Es posible configurar la seguridad del recurso asignando los permisos apropiados para cada rol de seguridad en cada vista organizativa. Además asigna los permisos apropiados en los grupos organizativos dentro de cada vista. Un permiso que se asigna a un grupo organizativo se aplica a todos los recursos en ese grupo. De forma predeterminada, el permiso se aplica a todos los grupos secundarios. No es posible asignar permisos directamente a un recurso determinado.

Los privilegios, permisos en carpetas y elementos, y los permisos en vistas y grupos organizativos trabajan conjuntamente. Necesita asignar la combinación apropiada para cada rol de seguridad a fin de otorgar el acceso que las cuentas de usuario necesitan para realizar sus actividades.

Ver "Configuración de la seguridad de Symantec Management Platform" en la página 85.

Ver "Tareas de administración de la seguridad de Symantec Management Platform" en la página 109.

Configuración de la seguridad de Symantec Management Platform

Para que las cuentas de usuario tengan acceso a Symantec Management Platform, las soluciones instaladas y los datos que se contienen en la CMDB, es necesario configurar los roles de seguridad. Se asignan los privilegios y los permisos

apropiados para cada rol. Es necesario crear las cuentas de usuario de Symantec Management Platform y después agregar cada cuenta de usuario al rol apropiado.

Ver "Acerca de la seguridad de Symantec Management Platform" en la página 84.

Tabla 4-1 Proceso para la configuración de la seguridad de Symantec Management Platform

Paso	Acción	Descripción
Paso 1	Cree y configure los roles de seguridad que se requieren.	Los roles de seguridad controlan el acceso a Symantec Management Platform, a la funcionalidad de la solución instalada y a todos los datos que se encuentran en la CMDB. Es posible crear nuevos roles de seguridad de las siguientes maneras: ■ Crear nuevos roles de seguridad. ■ Clone roles de seguridad existentes. ■ Importe los grupos y los usuarios de dominio de Active Directory. Ver "Creación y configuración de roles de seguridad" en la página 89.
Paso 2	Asigne los privilegios apropiados para sus roles de seguridad.	Un privilegio permite que un rol del miembro realice una acción determinada en Symantec Management Platform o en elementos en Symantec Management Console. Para realizar una acción en un elemento, el rol debe tener el permiso necesario en el elemento. Ver "Asignación de privilegios a un rol de seguridad" en la página 93.

Paso	Acción	Descripción
Paso 3	Cree y configure las cuentas de usuario que se requieren.	Cada cuenta de usuario de Symantec Management Platform contiene las credenciales que el usuario necesita para acceder a Symantec Management Console o para ejecutar un flujo de trabajo. Las credenciales pueden ser contraseñas y nombres de usuario internos de Symantec Management Platform o cuentas de Windows. Las credenciales internas se usan actualmente para la integración del flujo de trabajo solamente. Las credenciales de Windows son necesarias para acceder a Symantec Management Console. Es posible crear nuevas cuentas de usuario de las siguientes maneras: ■ Cree cuentas de usuario totalmente nuevas. ■ Clone cuentas de usuario existentes. ■ Importe los grupos y los usuarios de dominio de Active Directory. Ver "Creación y configuración de las cuentas de usuario Symantec Management Platform" en la página 225. Ver "Cómo especificar los detalles generales de la cuenta de usuario de Symantec Management Platform" en la página 98. Ver "Configuración de credenciales para una cuenta de usuario de Symantec Management Platform" en la página 99.
Paso 4	Agregue a los miembros a los roles de seguridad apropiados.	Un usuario accede a Symantec Management Platform, a las soluciones instaladas y a los datos que se contienen en la CMDB a través de la pertenencia de su rol de seguridad. Puede asignar un usuario a cualquier número de roles de seguridad. Un usuario que es miembro de varios roles de seguridad tiene la unión de todos los privilegios y los permisos que esos roles conceden. Ver "Adición de miembros a un rol de seguridad" en la página 101. Ver "Asignación de una cuenta de usuario de Symantec Management Platform a un rol de seguridad" en la página 102. Ver "Cómo agregar roles de seguridad como miembros de otros roles de seguridad" en la página 103.

Paso	Acción	Descripción
Paso 5	Para cada rol de seguridad, asigne los permisos en las carpetas y los elementos que se encuentran en Symantec Management Console.	Los permisos especifican el acceso que cada rol de seguridad tiene a una carpeta de Symantec Management Console o a un elemento determinado. Un permiso en un elemento se aplica solamente al elemento. Un permiso en una carpeta se aplica a todos los elementos que están contenidos directamente en esa carpeta. De forma predeterminada, el contenido de una carpeta hereda todos los permisos en la carpeta. Ver "Asignación de permisos de seguridad a carpetas y elementos" en la página 103.
Paso 6	(Opcional) Para cada rol de seguridad, modifique el permiso de herencia en la estructura de carpeta de Symantec Management Console.	Al modificar el permiso de herencia le permite personalizar los permisos en la estructura de carpeta de Symantec Management Console. Esto significa que se puede conceder un permiso determinado en una carpeta principal, pero eliminar ese permiso de alguno o de todos los contenidos de la carpeta. Recuerde que se configuran los permisos en las carpetas y los elementos dentro de esas carpetas. Si configura una carpeta y concede permisos de escritura para un rol determinado, ese rol tiene el permiso de escritura para la carpeta y todo su contenido. Si la carpeta contiene 100 elementos y usted no desea que esos elementos hereden el permiso de escritura de la carpeta principal, se puede finalizar la herencia de permisos. En ese caso, los usuarios que son miembros del rol al cual usted concedió el permiso de escritura tienen el permiso de escritura en la carpeta solamente. Sin embargo, no tienen el permiso de escritura en los elementos que la carpeta contiene. La herencia de permisos en una carpeta o un elemento se aplica a todos los roles de seguridad. No es posible personalizar la herencia de permisos por rol. Ver "Personalización de permisos de herencia" en la página 104.

Paso	Acción	Descripción
Paso 7	(Opcional) Configurar la seguridad del recurso.	De forma predeterminada, todos los roles de seguridad predefinidos tienen el permiso de lectura en los recursos. Los recursos relacionados con la seguridad son especialmente controlados en Symantec Management Platform: solamente los usuarios que son miembros del rol de administradores de Symantec tienen acceso total a los recursos de seguridad de forma predeterminada. Los usuarios que son miembros del rol de supervisores de Symantec tienen permisos de lectura en los recursos de seguridad de forma predeterminada. Ningún otro rol de seguridad predefinido tiene permisos en los recursos de seguridad. Ver "Roles de seguridad predefinidos" en la página 107. Si desea restringir o controlar el acceso a los recursos, puede configurar la seguridad de recursos. Puede crear la seguridad del recurso creando una o más vistas organizativas que modelen su estructura del recurso. Se controla el acceso a los recursos asignando permisos a cada rol de seguridad en las vistas y los grupos organizativos apropiados.

Creación y configuración de roles de seguridad

Un rol de seguridad es un conjunto de privilegios y permisos que se otorgan a todos los miembros del rol. El uso de seguridad basada en rol permite crear y mantener una pequeña cantidad de roles de seguridad y asignar a cada cuenta de usuario el rol apropiado. No es necesario asignar los privilegios y los permisos a cada cuenta de usuario individual. Es posible asignar una cuenta de usuario a varios roles de seguridad: un miembro de varios roles de seguridad tiene la unión de todos los privilegios y los permisos que esos roles conceden.

Ver "Acerca de la seguridad de Symantec Management Platform" en la página 84.

Los roles de seguridad pueden ser jerarquizados: un rol puede ser un miembro de uno o más roles y su pertenencia puede incluir roles y cuentas de usuario. La única restricción es que no se puede crear un rol circular de pertenencia donde un rol es miembro de sí mismo.

Los privilegios, permisos en carpetas y elementos, y los permisos en vistas y grupos organizativos trabajan conjuntamente. Necesita asignar la combinación apropiada para cada rol de seguridad a fin de otorgar el acceso que las cuentas de usuario necesitan para realizar sus actividades. Los privilegios pueden solamente asignarse a los roles de seguridad, pero los permisos pueden asignarse a los roles de seguridad y a las cuentas de usuario.

Debe decidir qué roles de seguridad se configurarán basándose en el trabajador de TI lógico o grupos de usuario en su organización. Por ejemplo, puede desear un rol de empleado de TI con nivel 1, un rol de administración con nivel superior y un rol de recursos humanos. Todas las cuentas de usuario en un rol de seguridad reciben los mismos privilegios y permisos y, por ende, tienen el mismo nivel de acceso a Symantec Management Platform.

Puede crear y configurar un rol de seguridad en una de las siguientes formas:

Cree un nuevo rol de seguridad o clone un rol de seguridad existente.	Symantec Management Platform y algunas soluciones incluyen roles de seguridad predefinidos. Ver "Roles de seguridad predefinidos" en la página 107. Si los roles de seguridad predefinidos no cubren las necesidades de su organización, se pueden crear nuevos roles o se pueden clonar los roles existentes para crear nuevos roles. Luego, es posible modificar los privilegios y los permisos según sea necesario. Ver "Para crear un nuevo rol de seguridad o clonar un rol de seguridad existente" en la página 91.
Importe los grupos y os usuarios de dominio con Active Directory.	Cuando se importan los grupos de dominio de Active Directory, un rol de seguridad se crea en el servidor de Symantec Management Platform para el grupo del dominio que desee importar. Los miembros de este grupo de dominio, incluidos los usuarios y los subgrupos, también se importan. Los usuarios se crean como cuentas, y los subgrupos se crean como roles. La relación de la pertenencia se conserva durante la importación. Ver "Para importar grupos y usuarios de dominio de Active Directory" en la página 92.

Durante la instalación de Symantec Management Platform, el administrador que está instalando Symantec Management Platform recibe automáticamente el rol de administrador de Symantec. El administrador puede entonces crear cualquier nuevo rol de seguridad que sea necesario y asignar a cada rol los privilegios y los permisos apropiados. El administrador puede entonces asignar a cada usuario uno o más roles.

Symantec recomienda configurar los roles de seguridad antes de que Notification Server se implemente en su red de producción.

Esta tarea es un paso en el proceso para configurar la seguridad de Symantec Management Platform.

Ver "Configuración de la seguridad de Symantec Management Platform" en la página 85.

Para crear un nuevo rol de seguridad o clonar un rol de seguridad existente

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Seguridad > Administración de cuentas**.
2. En el panel izquierdo, en **Administración de cuentas**, haga clic en **Roles**.
3. En la página **Roles**, en el panel izquierdo, elija una de las siguientes opciones:

Para crear un nuevo rol	Haga clic en **Agregar**. En el cuadro de diálogo **Nuevo rol**, escriba el nuevo nombre del rol de seguridad y después haga clic en **Aceptar**. El nuevo rol aparece en la lista de roles y la configuración predeterminada se muestra en el panel derecho.
Para clonar un rol existente	Seleccione el rol de seguridad que desee clonar. Haga clic con el botón derecho en el rol y haga clic en **Clonar**.

4. En el panel derecho, configure la opción apropiada en las fichas siguientes:

Miembros	Los roles y las cuentas de usuario que se asignan al rol. Un rol de pertenencia puede incluir cualquier número de cuentas de usuario y de roles. Los miembros de un rol tienen todos los privilegios y permisos que el rol concede. Ver "Adición de miembros a un rol de seguridad" en la página 101.
Miembro de	Los roles de seguridad a los cuales el rol pertenece. El rol tiene la unión de los permisos y de los privilegios de estos roles, combinados con cualquier permiso o privilegio adicional que se asigne directamente al rol. Ver "Cómo agregar roles de seguridad como miembros de otros roles de seguridad" en la página 103.
Privilegios	Los privilegios que el rol concede a sus miembros. Un privilegio permite que una cuenta de usuario realice una acción determinada en Symantec Management Platform o sobre elementos en Symantec Management Console. En algunos casos, la cuenta de usuario debe además tener un permiso correspondiente en el elemento. Ver "Asignación de privilegios a un rol de seguridad" en la página 93.

5 (Opcional) Si desea acceder al Administrador de roles de seguridad para ver o establecer permisos para el rol de seguridad, haga clic en **Mostrar la consola del Administrador del rol de seguridad**.

6 Haga clic en **Guardar cambios**.

Para importar grupos y usuarios de dominio de Active Directory

1 En Symantec Management Console, en el menú **Acciones**, haga clic en **Detectar > Importar Microsoft Active Directory**.

2 En la página **Importación de Microsoft Active Directory**, en la descripción que se etiqueta **Importar recursos de cuenta y roles de <origen de datos>, de (ninguno). Ejecute esta importación en las programaciones especificadas**, haga clic en el grupo de usuarios **(ninguno)**.

3 (Opcional) Cree su propias reglas de importación de roles y cuentas.

4 En el cuadro de diálogo **Seleccionar grupos de seguridad**, busque los grupos de dominio que desee agregar; por ejemplo, administradores y usuarios.

5 Haga clic en **Agregar** para agregar los grupos seleccionados y, después, haga clic en **Aceptar**.

6 Ejecute la regla como importación completa para importar el grupo de dominio seleccionado.

7 (Opcional) Se puede también programar una importación completa para que se ejecute en los intervalos apropiados.

Es posible usar esta programación para sincronizar su pertenencia al rol de seguridad con la pertenencia al grupo de dominio. Esto significa que si se quita un usuario de dominio del grupo de dominio, la cuenta de seguridad correspondiente se quita del rol de seguridad correspondiente. Asimismo, si se agrega un usuario de dominio al grupo de dominio, la cuenta de seguridad correspondiente se crea y se agrega el rol de seguridad correspondiente. Tenga en cuenta que si se quita un usuario de dominio de un grupo de dominio, la cuenta de seguridad correspondiente no se elimina. Solamente la pertenencia al rol de seguridad se quita.

8 En Symantec Management Console, en el menú **Configuración**, haga clic en **Seguridad > Administración de cuentas**.

9 En el panel izquierdo, en la carpeta **Administración de cuentas**, haga clic en **Roles** y, después, haga clic en el rol que desee editar.

10 (Opcional) En el panel derecho, configure la configuración apropiada en las fichas siguientes:

Miembros	Los roles y las cuentas de usuario que se asignan al rol. Un rol de pertenencia puede incluir cualquier número de cuentas de usuario y de roles. Los miembros de un rol tienen todos los privilegios y permisos que el rol concede. Ver "Adición de miembros a un rol de seguridad" en la página 101. Tenga en cuenta que no debe modificar manualmente los miembros de los roles que importó de Active Directory. Este obstáculo existe porque cualquier ejecución subsiguiente de la regla sobrescribe la configuración de la pertenencia. Los roles que se importan de Active Directory se diseñan para mantener la misma pertenencia que los grupos de dominio correspondientes.
Miembro de	Los roles de seguridad a los cuales el rol pertenece. El rol tiene la unión de los permisos y de los privilegios de estos roles, combinados con cualquier permiso o privilegio adicional que se asigne directamente al rol. Ver "Cómo agregar roles de seguridad como miembros de otros roles de seguridad" en la página 103.
Privilegios	Los privilegios que el rol concede a sus miembros. Un privilegio permite que una cuenta de usuario realice una acción determinada en Symantec Management Platform o en elementos en Symantec Management Console. En algunos casos, la cuenta de usuario debe además tener un permiso correspondiente en el elemento. Ver "Asignación de privilegios a un rol de seguridad" en la página 93.

11 (Opcional) Si desea acceder al Administrador de roles de seguridad para ver o establecer permisos para el rol de seguridad, haga clic en **Mostrar la consola del Administrador del rol de seguridad**.

12 Haga clic en **Guardar cambios**.

Asignación de privilegios a un rol de seguridad

Necesita especificar los privilegios que cada rol de seguridad les otorga a sus miembros. Un privilegio permite que un usuario realice una acción determinada en Symantec Management Platform o en elementos en Symantec Management

Console. Para realizar una acción en un elemento, el rol de usuario debe tener el permiso necesario sobre el elemento. Por ejemplo, si desea otorgar un rol a los privilegios Iniciar y Detener tarea, debe asignar el permiso de Ejecutar tarea al rol para las tareas apropiadas. El rol no tiene acceso a ninguna tarea que no tenga el permiso Ejecutar tarea asignado a ese rol.

Ver "Asignación de permisos de seguridad a carpetas y elementos" en la página 103.

La asignación de los privilegios a un rol de seguridad es parte de configurar los roles de seguridad. Esta tarea es un paso en el proceso de configurar la seguridad de Symantec Management Platform.

Ver "Creación y configuración de roles de seguridad" en la página 89.

Para asignar privilegios a un rol de seguridad

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Seguridad > Administración de cuentas**.
2. En el panel izquierdo, haga clic en **Administración de cuentas > Roles**.
3. En la página **Roles**, en el panel izquierdo, haga clic en el rol de seguridad que desee configurar.
4. En el panel derecho, en la ficha **Privilegios**, seleccione los privilegios que desee asignar al rol.

   Para seleccionar un privilegio, seleccione la casilla de selección correspondiente.

   Ver "Categorías de privilegios de seguridad" en la página 489.
5. Haga clic en **Guardar cambios**.

Creación y configuración de las cuentas de usuario Symantec Management Platform

Symantec Management Platform tiene sus propias cuentas de usuario. Las versiones anteriores a 7.1 de Symantec Management Platform usaban usuarios y grupos de Windows para la seguridad de usuario. Aún se usan los usuarios de Windows, pero ya no son el único mecanismo de seguridad.

Las cuentas de usuario, que a veces se denominan usuarios, no son lo mismo que recursos de usuario en Symantec Management Platform. Un recurso de usuario es una entidad que se usa para asociar los dispositivos administrados con el propietario del dispositivo. Los recursos de usuario existentes y las cuentas de usuario que pueden iniciar sesión en Symantec Management Console o ejecutar un flujo de trabajo son entidades individuales.

Una cuenta de usuario de Symantec Management Platform se enlaza a las credenciales de Windows que el usuario necesita para acceder a Symantec Management Console. La cuenta de usuario se puede además vincular a las credenciales internas que puede usar para acceder a otros servicios de Symantec Management Platform, tales como flujos de trabajo. La cuenta de usuario se puede agregar a los roles de seguridad apropiados: una cuenta tiene la unión de todos los privilegios y los permisos concedidos por los roles a los cuales pertenece.

Una credencial es algo que una cuenta de usuario proporciona para probar su identidad. En Symantec Management Platform, una credencial puede ser un nombre de usuario y una contraseña o una cuenta de Windows. La cuenta de usuario asocia una o más credenciales a un usuario determinado y permite el acceso de usuario a Symantec Management Console o a los servicios de Symantec Management Platform.

Symantec Management Platform usa dos tipos de credenciales:

Credencial interna	Permite un acceso de usuario a los servidores de Symantec Management Platform apropiados con un nombre de usuario y una contraseña que se almacenan en la CMDB. Por razones de seguridad, solamente el valor de hash de la contraseña se almacena. Una cuenta de usuario no puede usar las credenciales internas para acceder a Symantec Management Console. Las credenciales internas se usan actualmente solo para la integración del flujo de trabajo.
Credencial de Windows	Permite a un usuario acceder a Symantec Management Console y a los servicios de Symantec Management Platform que usan un nombre y una contraseña de usuario de Windows. Para usar las credenciales de Windows, Notification Server debe estar en el dominio del usuario o el dominio de Notification Server debe confiar en el dominio del usuario. Es necesario configurar las credenciales de Windows si su organización usa las cuentas de Windows internamente. El uso de las credenciales de Windows le permite exigir los requisitos de complejidad de la contraseña, cambiar periódicamente contraseñas, guardar el historial de la contraseña y realizar otras tareas de administración de contraseñas en Windows.

Es posible configurar sus cuentas de usuario de Symantec Management Platform para cumplir con los requisitos de su organización. Es necesario crear todas las cuentas que desee y asignarlas a los roles de seguridad apropiados. Cada cuenta tiene la unión de todos los privilegios y permisos que los roles a los cuales pertenece le conceden.

Es posible crear y configurar una cuenta de usuario de una de las siguientes formas:

- Cree una cuenta de usuario nueva o clone una cuenta de usuario existente.
- Importe los grupos y los usuarios de dominio de Active Directory.

Esta tarea es un paso en el proceso para configurar la seguridad de Symantec Management Platform.

Ver "Configuración de la seguridad de Symantec Management Platform" en la página 85.

Para crear una cuenta de usuario nueva o clonar una cuenta de usuario existente

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Seguridad > Administración de cuentas**.
2. En el panel izquierdo, haga clic en **Administración de cuentas > Cuentas**.
3. En la página **Cuentas**, en el panel izquierdo, realice una de las siguientes acciones:

Para crear una nueva cuenta	Haga clic en **Agregar**. En el cuadro de diálogo **Cuenta nueva**, escriba el nuevo nombre de cuenta de Symantec Management Platform y después haga clic en **Aceptar**. La nueva cuenta aparece en la lista de cuentas. De forma predeterminada, el nuevo estado de cuenta es Inactivo.
Para clonar una cuenta existente	Haga clic con el botón derecho en la cuenta de Symantec Management Platform que desee clonar y configurar. Escriba el nombre de la nueva copia de esta cuenta y haga clic en **Aceptar**.

4 En el panel derecho, configure la opción apropiada en las fichas siguientes:

General	Los detalles de la cuenta general. Estos incluyen el nombre completo y la dirección de correo electrónico del usuario para quien se crea la cuenta, el estado de cuenta y las credenciales de la cuenta. Ver "Cómo especificar los detalles generales de la cuenta de usuario de Symantec Management Platform" en la página 98. Ver "Configuración de credenciales para una cuenta de usuario de Symantec Management Platform" en la página 99.
Miembro de	Los roles de seguridad a los cuales la cuenta pertenece. La cuenta tiene la unión de todos los privilegios y permisos que los roles a los cuales pertenece le conceden. Ver "Asignación de una cuenta de usuario de Symantec Management Platform a un rol de seguridad" en la página 102.

5 Haga clic en **Guardar cambios**.

Para importar grupos y usuarios de dominio de Active Directory

1 En Symantec Management Console, en el menú **Acciones**, haga clic en **Detectar > Importar Microsoft Active Directory**.

2 En la página **Importación de Microsoft Active Directory**, en la descripción que se etiqueta **Importar recursos de cuenta y roles de <origen de datos>, de (ninguno). Ejecute esta importación en las programaciones especificadas.**, haga clic en el grupo de usuarios **(ninguno)**.

3 (Opcional) Cree su propias reglas de importación de roles y cuentas.

4 En el cuadro de diálogo **Seleccionar grupos de seguridad**, busque los grupos de dominio de los que desee importar cuentas de usuario; por ejemplo, Administradores y Usuarios.

5 Haga clic en **Agregar** y, a continuación, en **Aceptar** para agregar los grupos seleccionados.

6 Ejecute la regla como importación completa para importar los grupos de dominio seleccionados.

7 (Opcional) Se puede también programar una importación completa para que se ejecute en los intervalos apropiados.

Es posible usar esta programación para sincronizar su pertenencia al rol de seguridad con la pertenencia al grupo de dominio. Esto significa que si se quita un usuario de dominio del grupo de dominio, la cuenta de seguridad correspondiente se quita del rol de seguridad correspondiente. Asimismo, si se agrega un usuario de dominio al grupo de dominio, la cuenta de seguridad correspondiente se crea y se agrega el rol de seguridad correspondiente. Tenga en cuenta que si se quita un usuario de dominio de un grupo de dominio, la cuenta de seguridad correspondiente no se elimina. Solamente la pertenencia al rol de seguridad se quita.

Video: Para obtener más información acerca de crear las cuentas de usuario Symantec Management Platform, consulte el video Creating a Limited ITMS Administrator Role (Creación de un rol de administrador de ITMS limitado) en Symantec Connect.

Cómo especificar los detalles generales de la cuenta de usuario de Symantec Management Platform

Es necesario especificar el nombre completo y la dirección de correo electrónico del usuario para quien se crea la cuenta. Es posible también cambiar el estado de cuenta de Inactiva a Activa cuando corresponda.

Ver "Creación y configuración de las cuentas de usuario Symantec Management Platform" en la página 225.

Para especificar los detalles generales de la cuenta de usuario de Symantec Management Platform

1 En Symantec Management Console, en el menú **Configuración**, haga clic en **Seguridad > Administración de cuentas**.

2 En el panel izquierdo, haga clic en **Administración de cuentas > Cuentas**.

3 En la página **Cuentas**, en el panel izquierdo, haga clic en la cuenta que desee configurar.

4 En el panel derecho, en la ficha **General**, especifique los detalles de la cuenta editando los cuadros apropiados:

Nombre completo	El nombre completo del usuario a quien la cuenta pertenece.
Correo electrónico	La dirección de correo electrónico del usuario de la cuenta.

5 (Opcional) Si desea activar o desactivar la cuenta, haga clic en el icono de estado en la barra de título y después seleccione **Activo** o **Inactivo**.

6 Haga clic en **Guardar cambios**.

Configuración de credenciales para una cuenta de usuario de Symantec Management Platform

Es necesario configurar las credenciales apropiadas para cada cuenta de usuario de Symantec Management Platform. Es posible agregar una credencial interna de Symantec Management Platform y una credencial de Windows a una cuenta de usuario. La credencial de Windows emula el comportamiento de versiones anteriores de Symantec Management Platform.

Una credencial interna permite un acceso de usuario a los servidores de Symantec Management Platform apropiados con un nombre de usuario y una contraseña que se almacenan en la CMDB. Actualmente, las credenciales internas se usan solamente para la integración del flujo de trabajo.

Una credencial de Windows permite que una cuenta de usuario acceda a Symantec Management Console y a los servicios de Symantec Management Platform que usan un nombre y una contraseña de usuario de Windows. Para usar las credenciales de Windows, Notification Server debe estar en el dominio del usuario o el dominio de Notification Server debe confiar en el dominio del usuario.

Es necesario configurar las credenciales de Windows si su organización usa las cuentas de Windows internamente. El uso de las credenciales de Windows le permite exigir los requisitos de complejidad de la contraseña, cambiar periódicamente contraseñas, guardar el historial de la contraseña y realizar otras tareas de administración de contraseñas en Windows.

Ver "Creación y configuración de las cuentas de usuario Symantec Management Platform" en la página 225.

Para configurar credenciales para una cuenta de usuario de Symantec Management Platform

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Seguridad > Administración de cuentas**.
2. En el panel izquierdo, haga clic en **Administración de cuentas > Cuentas**.
3. En la página **Cuentas**, en el panel izquierdo, haga clic en la cuenta que desee configurar.
4. En el panel derecho, en la ficha **General**, en **Credenciales**, haga clic en **Agregar credencial** y a continuación realice una de las siguientes acciones:

Para agregar una credencial de Windows a la cuenta	Haga clic en **Windows** y, a continuación, en el cuadro de diálogo **Credencial de Windows**, especifique el nombre de usuario de Windows apropiado en el formato dominio/nombre de usuario. Si la cuenta de Windows está en el mismo dominio que Notification Server, se puede omitir el dominio y especificar el nombre de usuario solamente. Si especifica una cuenta de Windows que ya está asignada a una cuenta de usuario, la credencial de Windows se quita de la cuenta existente. La credencial de Windows se agrega a la cuenta de usuario.
Para agregar una credencial interna a la cuenta	Haga clic en **Interno** y a continuación, en el cuadro de diálogo **Crear credencial interna**, especifique la contraseña apropiada. La contraseña debe cumplir con la configuración de complejidad de la contraseña. Ver "Configuración de la complejidad y del bloqueo de la contraseña" en la página 110. El nombre de usuario de la credencial es el nombre de la cuenta de Symantec Management Platform y no se puede cambiar.

5. Haga clic en **Aceptar**.

   La nueva credencial se agrega a la lista **Credenciales**.

6 (Opcional) Si desea modificar una credencial, selecciónela en la lista **Credenciales** y después haga clic en **Editar**. En el cuadro de diálogo **Editar credencial de Windows** o el cuadro de diálogo **Editar credencial interna**, realice los cambios apropiados y después haga clic en **Aceptar**.

   Por razones de seguridad, el cuadro de diálogo **Editar credencial interna** no muestra la contraseña actual. Si especifica una nueva contraseña, la credencial se actualiza según corresponda. Si deja el cuadro **Contraseña** vacío, se conserva la contraseña original.

7 (Opcional) Si desea eliminar una credencial, selecciónela en la lista **Credenciales** y después haga clic en **Eliminar**.

8 Haga clic en **Guardar cambios**.

Adición de miembros a un rol de seguridad

Es necesario asignar los miembros apropiados (cuentas de usuario y otros roles de seguridad) a cada uno de sus roles de seguridad. Es necesario ser un miembro del rol de administradores de Symantec o un miembro de un rol que tenga el privilegio Cambiar seguridad para agregar miembros. Puede asignar una cuenta de usuario a cualquier número de roles de seguridad. Los miembros de un rol tienen todos los privilegios y permisos que se conceden al rol.

Es posible agregar un rol a varios roles de seguridad, pero no se puede crear una pertenencia circular donde un rol determinado sea miembro de sí mismo. Un miembro de varios roles de seguridad tiene la unión de todos los privilegios y los permisos que esos roles conceden.

Agregar miembros a un rol de seguridad es parte de configurar los roles de seguridad. Esta tarea es un paso en el proceso para configurar la seguridad de Symantec Management Platform.

Ver "Creación y configuración de roles de seguridad" en la página 89.

Para agregar miembros a un rol de seguridad

1 En Symantec Management Console, en el menú **Configuración**, haga clic en **Seguridad > Administración de cuentas**.

2 En el panel izquierdo, haga clic en **Administración de cuentas > Roles**.

3 En la página **Roles**, en el panel izquierdo, haga clic en el rol de seguridad que desee configurar.

4 En el panel derecho, en la ficha **Miembros**, haga clic en **Agregar miembro** y después realice una de las siguientes opciones:

Para agregar una cuenta de usuario al rol	Haga clic en **Agregar cuenta**.
Para agregar otro rol de seguridad al rol	Haga clic en **Agregar rol**.

5 En el cuadro de diálogo **Seleccionar cuentas** o **Seleccionar roles**, seleccione las cuentas de usuario o los roles de seguridad que desee agregar y después haga clic en **Aceptar**.

6 En la ficha **Miembros**, verifique que la lista de usuarios sea correcta. Puede eliminar cualquiera de las listas que no desee.

7 Haga clic en **Guardar cambios**.

Asignación de una cuenta de usuario de Symantec Management Platform a un rol de seguridad

Es necesario asignar cada cuenta de usuario de Symantec Management Platform a los roles de seguridad apropiados. Es necesario ser miembro del rol de administradores de Symantec o miembro de un rol que tenga el privilegio Cambiar seguridad para asignar roles de pertenencia. La cuenta tiene la unión de todos los privilegios y permisos que los roles a los cuales pertenece le conceden.

Ver "Creación y configuración de las cuentas de usuario Symantec Management Platform" en la página 225.

Para asignar Symantec Management Platform a un rol de seguridad

1 En Symantec Management Console, en el menú **Configuración**, haga clic en **Seguridad > Administración de cuentas**.

2 En el panel izquierdo, haga clic en **Administración de cuentas > Cuentas**.

3 En la página **Cuentas**, en el panel izquierdo, haga clic en la cuenta que desee configurar.

4 En el panel derecho, en la ficha **Miembro de**, realice la configuración apropiada.

5 Haga clic en **Agregar rol**.

6 En el cuadro de diálogo **Seleccionar roles**, seleccione los roles de seguridad a los cuales desee agregar la cuenta y, a continuación, haga clic en **Aceptar**.

7 En la ficha **Miembro de**, verifique que la lista de roles de seguridad sea correcta. Puede eliminar cualquiera de las listas que no desee.

8 Haga clic en **Guardar cambios**.

Cómo agregar roles de seguridad como miembros de otros roles de seguridad

Es posible agregar un rol como miembro de otros roles de seguridad. Es necesario ser miembro del rol de administradores de Symantec o miembro de un rol que tenga el privilegio Cambiar seguridad para asignar roles de pertenencia. Es posible agregar un rol a varios roles de seguridad, pero no se puede crear una pertenencia circular donde un rol determinado sea miembro de sí mismo. Al rol se le concede la unión de todos los privilegios y los permisos que los roles a los cuales pertenece proporcionan.

Agregar un rol como miembro de otro rol es lo mismo que el otro rol agregue el rol a su pertenencia. Este método le permite agregar un rol determinado a varios roles en un único procedimiento. La alternativa sería configurar todos los otros roles y agregar específicamente el rol a la pertenencia de cada uno.

Agregar los roles de seguridad como miembros de otros roles de seguridad es parte de configurar los roles de seguridad. Esta tarea es un paso en el proceso de configurar la seguridad de Symantec Management Platform.

Ver "Creación y configuración de roles de seguridad" en la página 89.

Para agregar un rol de seguridad como miembro de otros roles de seguridad

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Seguridad > Administración de cuentas**.
2. En el panel izquierdo, haga clic en **Administración de cuentas > Roles**.
3. En la página **Roles**, en el panel izquierdo, haga clic en el rol de seguridad que desee configurar.
4. En el panel derecho, en la ficha **Miembro de**, realice la configuración apropiada.
5. Haga clic en **Agregar rol**.
6. En el cuadro de diálogo **Seleccionar roles**, seleccione los roles de seguridad a los cuales desee agregar el rol y, a continuación, haga clic en **Aceptar**.
7. En la ficha **Miembro de**, verifique que la lista de roles de seguridad sea correcta. Puede eliminar cualquiera de las listas que no desee.
8. Haga clic en **Guardar cambios**.

Asignación de permisos de seguridad a carpetas y elementos

Puede especificar los permisos no heredados que se aplican a cada carpeta o elemento para cada rol de seguridad. Estos se combinan con los permisos que se heredan de la carpeta principal. Los permisos combinados determinan el acceso que tiene el rol de seguridad a esa carpeta o ese elemento en particular. De forma

predeterminada, cualquier carpeta o elemento secundario hereda el conjunto de permisos combinados.

Ver "Acceso al Administrador de roles de seguridad" en la página 113.

Esta tarea es un paso en el proceso para configurar la seguridad de Symantec Management Platform.

Ver "Configuración de la seguridad de Symantec Management Platform" en la página 85.

Para asignar permisos de seguridad a carpetas y elementos

1. En el Administrador de roles de seguridad, en la lista desplegable **Rol**, seleccione el rol de seguridad para el cual desea configurar permisos.
2. (Opcional) En la lista desplegable **Ver**, seleccione una categoría de elemento para ver la estructura de la carpeta que contiene los elementos relevantes.

   Si desea ver la estructura completa de la carpeta, seleccione **Todos los elementos**.
3. En el panel izquierdo, seleccione la carpeta o el elemento para el cual desea configurar permisos.

   Tenga en cuenta que algunos elementos pueden estar ocultos de forma predeterminada. Para ver todos los elementos, haga clic en el icono **Mostrar elementos ocultos** en la barra de herramientas. Esta funcionalidad solamente está disponible para los roles que tienen el privilegio **Cambiar seguridad** asignado a ellos.

   Advertencia: Sea cuidadoso al editar los permisos de seguridad de un elemento oculto, porque no se diseñan para ser modificados.

   ---
4. En el panel derecho, en el panel **No heredado**, realice los cambios apropiados para configurar permisos.
5. (Opcional) Si desea configurar la herencia de permisos para esta carpeta o elemento, haga clic en **Opciones avanzadas**.

   Ver "Personalización de permisos de herencia" en la página 104.
6. Haga clic en **Guardar cambios**.

Personalización de permisos de herencia

De manera predeterminada, el permiso de herencia se habilita para todas las carpetas y elementos. Las carpetas secundarias y los elementos heredan los permisos de seguridad para cada rol que se asigne a una carpeta. Los permisos

heredados no se pueden modificar en las carpetas secundarias y sus elementos. Sin embargo, se pueden especificar permisos no heredados adicionales. Los permisos no heredados se aplican directamente a la carpeta o el elemento y se pueden modificar en cualquier momento. La configuración de permisos en cada carpeta o elemento es la combinación de configuración de los permisos heredados y de los no heredados. El conjunto combinado de permisos entonces se aplica a cualquier carpeta secundaria o elemento. Cualquier modificación en la configuración de permisos para una carpeta se aplica de manera inmediata a todas las carpetas secundarias y sus elementos.

Puede deshabilitar el permiso de herencia para cualquier carpeta o elemento. Esto le permite eliminar algunos de los permisos heredados de la carpeta o del elemento y conservarlos en su carpeta principal. La configuración de la herencia de permisos que usted aplica a una carpeta o a un elemento se aplica a cada rol de seguridad. No se puede personalizar la configuración de la herencia para roles particulares.

Advertencia: Al deshabilitar las herencias de permisos en una carpeta o elemento, puede generar una denegación de acceso inesperada para las cuentas de usuario. Si deshabilita la herencia de permisos, asegúrese de que haya permisos explícitamente especificados en la carpeta o el elemento para que las cuentas de usuario tengan el acceso apropiado.

También puede eliminar todos los permisos no heredados de carpetas o elementos dejando solamente los permisos heredados. Es conveniente eliminar todos los permisos no heredados para eliminar los permisos personalizados que se han agregado a las carpetas secundarias o a los elementos. Es posible también usar esta función para restaurar un conjunto estándar de permisos en todas las carpetas secundarias y los elementos.

Ver "Asignación de permisos de seguridad a carpetas y elementos" en la página 103.

Esta tarea es un paso en el proceso para configurar la seguridad de Symantec Management Platform.

Ver "Configuración de la seguridad de Symantec Management Platform" en la página 85.

Para personalizar permisos de herencia para una carpeta o elemento

1. En el Administrador de roles de seguridad, en el panel izquierdo, seleccione la carpeta o elemento para el cual desea configurar el permiso de herencia.
2. En el panel derecho, haga clic en **Opciones avanzadas**.

3 En la ventana Permisos para: En la ventana *Nombre del elemento*, en la lista **Cuenta/Grupo/Rol**, seleccione el rol de seguridad o la cuenta de usuario para los cuales desee configurar los permisos.

Si desea agregar otro rol de seguridad o cuenta de usuario a la lista, haga clic en **Agregar**. En la ventana **Agregar elementos de confianza**, elija el rol de seguridad o la cuenta de usuario apropiados.

4 (Opcional) En el panel **Permisos para**, cambie los permisos que están asignados al rol de seguridad para esta carpeta o elemento.

Puede utilizar esta función solamente para los permisos no heredados. No puede editar los permisos heredados.

5 Realice cualquiera de las siguientes opciones:

Para heredar permisos de la carpeta principal	Seleccione **Heredar del objeto principal de las entradas de permisos aplicables a los objetos secundarios**. La configuración del permiso heredado en la carpeta o elemento se actualiza para poder así reflejar la configuración del permiso actual en la carpeta principal.
Para deshabilitar los permisos de herencia	Anule la selección de **Heredar del objeto principal de las entradas de permisos aplicables a los objetos secundarios**. Cuenta con la opción de copiar los permisos heredados actuales de la carpeta principal o de eliminar todos los permisos heredados. Cualquier cambio subsiguiente a la configuración de permiso en la carpeta principal no afectará la configuración de permiso en la carpeta o el elemento.
Para quitar todos los permisos no heredados de las carpetas o los elementos secundarios	Seleccione **Reemplazar los permisos en todos los objetos secundarios**. Se borra la configuración de permisos no heredados en carpetas y elementos secundarios dejando sólo los permisos heredados.

6 Haga clic en **Guardar cambios**.

7 (Opcional) Si deshabilitó los permisos de herencia, en el cuadro de diálogo **Comportamiento de los permisos heredados**, haga clic en la opción apropiada:

Copiar	Los permisos heredados actuales se combinan con la configuración de los permisos no heredados en esta carpeta o elemento.
Quitar	Se borran los permisos heredados actuales dejando sólo los permisos no heredados. Asegúrese de que tenga los permisos heredados apropiados en la carpeta o el elemento antes de que seleccione esta opción.

8 Haga clic en **Cancelar** para cerrar la ventana Permisos para: *Nombre del elemento*.

Roles de seguridad predefinidos

La Plataforma de administración Symantec incluye un conjunto de roles de seguridad predefinidos para usar. Si los roles de seguridad predefinidos no cumplen con los requerimientos de su organización, puede crear roles nuevos. Puede también editar los roles de seguridad predefinidos especificando los diferentes privilegios y permisos.

Ver "Creación y configuración de roles de seguridad" en la página 89.

Tabla 4-2 Roles de seguridad predefinidos de la Plataforma de administración Symantec

Rol de seguridad	Descripción
Todos	Un rol de nivel superior que contiene todos los roles y las cuentas de usuario. La pertenencia de este rol se calcula automáticamente y no se puede modificar manualmente. De forma predeterminada, este rol no tiene ningún privilegio asignado. Cuando se cambian los permisos y los privilegios para este rol, los cambios se aplican de forma automática a todos los demás roles y cuentas de usuario.
Administradores Symantec	Se les asignan todos los privilegios y permisos de seguridad, de modo que tienen acceso total a todos los aspectos de la Plataforma de administración Symantec y a cualquier solución instalada. Es posible modificar la pertenencia de este rol de seguridad, pero no se pueden cambiar sus privilegios y permisos.

Rol de seguridad	Descripción
Supervisores de Symantec	Tiene la administración completa y la mayoría de los privilegios del menú contextual. Tiene asignados privilegios del sistema limitados. Tiene el permiso de lectura en los recursos, incluidos los recursos de seguridad. Tiene el acceso completo a la configuración de administración habilitada para la nube, incluida la configuración de un nuevo gateway de Internet y la generación del paquete de instalación de Symantec Management Agent.
Trabajadores del nivel 2 de Symantec	Tiene los privilegios de administración completos y la mayoría de los privilegios del menú contextual asignados. Tiene el permiso de lectura en los recursos, excepto los recursos de seguridad. Tiene el acceso limitado a la configuración de administración habilitada para la nube. Por ejemplo, empleados de Symantec Nivel 2 pueden crear una política de **Configuración de Administración habilitada para la nube**.
Trabajadores del nivel 1 de Symantec	No se les asigna ningún privilegio. Tiene el permiso de lectura en los recursos, excepto los recursos de seguridad.
Bibliotecario de software de Symantec	Tiene los privilegios de Software Management Framework y los privilegios de las acciones del menú contextual asignados. Los privilegios se limitan a aquellos que son necesarios para crear y administrar paquetes de software.
Invitados de Symantec	No se les asigna ningún privilegio. Tiene el permiso de lectura en los informes.
NT Authority\Usuarios autenticados	Cualquier usuario que inicie sesión en Symantec Management Console, de forma automática, se convierte en miembro de este rol. La pertenencia de este rol se calcula automáticamente y no se puede modificar manualmente. De forma predeterminada, este rol no tiene privilegios ni permisos asignados.

Tareas de administración de la seguridad de Symantec Management Platform

Tabla 4-3 Tareas de administración de la seguridad de Symantec Management Platform

Tarea	Descripción
Establezca la configuración de la complejidad y del bloqueo de la contraseña.	Se pueden especificar requisitos apropiados de la complejidad de la contraseña para evitar que las cuentas de usuario de Symantec Management Platform creen contraseñas poco seguras. Los cambios que se realizan en la configuración de la complejidad de la contraseña no afectan las contraseñas existentes. Se aplican las reglas de la complejidad de la contraseña solamente cuando se crean o se cambian las contraseñas. Ver "Configuración de la complejidad y del bloqueo de la contraseña" en la página 110.
Desbloquee las credenciales.	Es posible desbloquear credenciales internas que se han bloqueado una vez que el número máximo de intentos de inicio de sesión incorrectos se ha excedido. Ver "Cómo desbloquear las credenciales" en la página 113.
Vea y administre los permisos de los roles de seguridad.	El Administrador de roles de seguridad le permite ver y configurar los permisos para los roles de seguridad. Puede utilizar también el Administrador de roles de seguridad para asumir la posesión de un elemento. Ver "Acceso al Administrador de roles de seguridad" en la página 113.
Asuma la posesión de una carpeta o elemento.	Es posible asumir la posesión de un elemento si sus permisos se quitan accidentalmente y el propietario ya no puede acceder a él. Una vez que se asume la posesión, se pueden restablecer los permisos apropiados y restaurar el acceso al propietario original. Ver "Propiedad de una carpeta o elemento" en la página 115.

Tarea	Descripción
Administre las credenciales.	Las soluciones de administración crean típicamente credenciales cuando son necesarias para realizar una tarea. Ver "Cómo administrar credenciales" en la página 115.

Configuración de la complejidad y del bloqueo de la contraseña

La página **Configuración de contraseña** le permite configurar la complejidad y el bloqueo de la contraseña de las credenciales internas. Esta configuración se aplica a las credenciales internas solamente: no se aplica a las contraseñas que se administran externamente, por ejemplo una cuenta de Windows. Esta configuración de complejidad y bloqueo se necesita a menudo para cumplir con la política del control de acceso de una organización.

Es necesario especificar requisitos apropiados de complejidad de contraseña para evitar que las cuentas de usuario de Symantec Management Platform creen contraseñas poco seguras.

Nota: Los cambios que se realizan en la configuración de la complejidad de la contraseña no afectan las contraseñas existentes. Se aplican las reglas de la complejidad de la contraseña solamente cuando se crean o se cambian las contraseñas.

No es posible especificar restricciones temporales tales como permitir que las cuentas de usuario inicien sesión solamente durante ciertos períodos o en días de la semana determinados. Para configurar este tipo de restricción, se puede usar una tarea programada, un flujo de trabajo o una política de automatización que deshabilite y habilite cuentas en los tiempos apropiados.

No es posible configurar la antigüedad máxima de la contraseña para las credenciales internas. La antigüedad máxima de la contraseña para las credenciales de Windows debe administrarse usando una política de Windows.

Ver "Cómo desbloquear las credenciales" en la página 113.

Es necesario especificar condiciones apropiadas del bloqueo de la contraseña para evitar acceso no autorizado a Symantec Management Platform. Cualquier cambio que se realice a la configuración del bloqueo de la contraseña se aplica a todos los intentos subsiguientes de inicio de sesión fallidos. La configuración de Intentos incorrectos máximos permitidos no se aplica al número de intentos anteriores de inicio de sesión fallidos.

Para establecer la configuración de la complejidad y del bloqueo de la contraseña

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Seguridad > Administración de cuentas**.
2. En el panel izquierdo, haga clic en **Administración de cuentas > Configuración de contraseña**.
3. En la página **Configuración de contraseña**, en la ficha **Complejidad de contraseña**, establezca la configuración de la complejidad de contraseña:

Permitir contraseña en blanco	Le permite especificar si una credencial puede tener una contraseña vacía. Si habilita esta configuración, se deshabilita la longitud mínima de la contraseña. De forma predeterminada, esta configuración está deshabilitada.
Longitud de contraseña mínima	Le permite especificar el número mínimo de caracteres que la contraseña debe contener. Si desea configurar la longitud en cero (0), se debe además habilitar la configuración de **Permitir contraseña en blanco**. El valor predeterminado es seis (6).
Cantidad mínima de caracteres no alfabéticos	Le permite especificar el número mínimo de caracteres no alfabéticos que la contraseña debe contener. Los caracteres no alfabéticos son números (como 1, 2, 3, etc.) y caracteres especiales (por ejemplo, ! ?, &, etc.). El valor predeterminado es uno (1).
Contiene el nombre de la cuenta	Le permite especificar si la contraseña puede contener el nombre de la cuenta de usuario. Tenga en cuenta que este parámetro no distingue mayúsculas y minúsculas. De forma predeterminada, esta configuración está deshabilitada.

4 En la página **Configuración de contraseña**, en la ficha **Bloqueo de contraseña**, especifique las condiciones apropiadas del bloqueo de la contraseña:

Habilitar bloqueo de credenciales

Especifica si se bloquearán las credenciales cuando el número máximo especificado de intentos de inicio de sesión incorrectos se alcance.

De forma predeterminada, esta configuración está habilitada.

Umbral de bloqueo de credenciales internas

Especifica el número máximo de intentos de inicio de sesión que un usuario puede hacer con cualquier credencial determinada. Si un usuario intenta autenticarse con una contraseña incorrecta una cantidad de veces mayor que este número, la credencial se bloquea durante el período especificado.

Los intentos de inicio de sesión incorrectos se cuentan a partir de que se crea la credencial. Los intentos fallidos no necesitan suceder dentro de un período mínimo. No hay hora máxima después de la cual ya no se cuente un intento fallido.

Si cambia esta configuración para reducir el número máximo de intentos incorrectos permitidos, el nuevo valor no se aplica a ninguna cuenta hasta que se realiza el intento de inicio de sesión siguiente. Si el intento siguiente es correcto, la cantidad se restablece en cero (se borran todos los errores anteriores). Sin embargo, si el intento siguiente falla, la cantidad de intentos fallidos se evalúa. Si se alcanza (o se excede) el número máximo, la cuenta se bloquea.

Duración de bloqueo

Especifica el tiempo durante el cual una credencial bloqueada no se puede usar. El período predeterminado es 1800 minutos (30 horas).

Todos los intentos de inicio de sesión que el usuario realiza en este período fracasan, incluso si se proporcionan las credenciales correctas. Cuando el período de bloqueo caduca, las mismas credenciales son válidas de nuevo. La restauración automática de la contraseña no es necesaria.

Es posible especificar un período infinito de bloqueo incorporando un valor de -1. En esta situación, una credencial bloqueada sigue siendo bloqueada hasta que un administrador desbloquea manualmente la credencial.

Ver "Cómo desbloquear las credenciales" en la página 113.

5 Haga clic en **Guardar cambios**.

Ver "Tareas de administración de la seguridad de Symantec Management Platform" en la página 109.

Cómo desbloquear las credenciales

La página **Desbloquear credenciales** le permite desbloquear las credenciales internas que se hayan bloqueado una vez que el número máximo de intentos de inicio de sesión incorrectos se haya excedido.

Ver "Configuración de la complejidad y del bloqueo de la contraseña" en la página 110.

Para desbloquear las credenciales bloqueadas

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Seguridad > Administración de cuentas**.
2. En el panel izquierdo, haga clic en **Administración de cuentas > Desbloquear credenciales**.
3. En la página **Desbloquear credenciales**, en la lista de credenciales bloqueadas, seleccione la credencial que desea desbloquear.
4. Haga clic en **Desbloquear credenciales**.

Acceso al Administrador de roles de seguridad

El Administrador de roles de seguridad es una consola especial que le permite ver y establecer permisos para los roles de seguridad. La consola le permite seleccionar un rol de seguridad en particular y ver los permisos que están asociados con cada elemento para ese rol de seguridad. Puede ver los elementos por tipo, o puede ver todos los elementos disponibles y seleccionar la carpeta o elemento en los cuales desea ver o establecer permisos. De forma predeterminada, las carpetas y los elementos secundarios heredan todos los permisos en una carpeta. Es posible modificar la herencia de permisos para adaptarse a sus requisitos.

Puede utilizar también el Administrador de roles de seguridad para asumir propiedad de un elemento. Es posible que sea necesario tomar propiedad si se quitan accidentalmente los permisos en un elemento de modo que el propietario ya no tenga acceso a él. Al asumir la posesión de un elemento, puede restablecer los permisos apropiados y restaurar el acceso para el propietario original.

Tabla 4-4 Maneras de acceder al Administrador de roles de seguridad

Opción	Descripción
Desde el menú **Configuración** de Symantec Management Console.	El Administrador de roles de seguridad se abre junto con el rol de seguridad seleccionado y se muestra la vista **Todas las clases de datos**.
Desde el panel derecho de la página **Roles**.	El Administrador de roles de seguridad se abre junto con el rol de seguridad apropiado que ha sido seleccionado y se muestra la vista **Todas las clases de datos**.
Desde el menú **Acciones** para un rol de seguridad.	El Administrador de roles de seguridad se abre junto con el rol de seguridad apropiado que ha sido seleccionado y se muestra la vista **Todas las clases de datos**.
Desde el menú contextual para un elemento o carpeta en el panel izquierdo.	Generalmente, debería usar este método para establecer los permisos en un elemento o una carpeta en particular. El administrador de roles de seguridad se abre junto con el rol de seguridad seleccionado y la carpeta apropiada que ha sido seleccionada.

Para acceder al administrador de roles de seguridad desde el menú de Symantec Management Console

- En Symantec Management Console, en el menú **Configuración**, haga clic en **Seguridad > Permisos**.

Para acceder al administrador de roles de seguridad para un rol de seguridad específico

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Seguridad > Administración de cuentas**.
2. En el panel izquierdo, haga clic en **Administración de cuentas > Roles**.
3. En la página **Roles**, en el panel izquierdo, haga clic en el rol de seguridad que desee configurar.
4. Realice una de las siguientes acciones:
   - En el panel derecho, haga clic en **Mostrar la Consola del Administrador del rol de seguridad**.
   - Haga clic en **Acciones > Administrador de roles de seguridad**.
   - Haga clic con el botón derecho en el rol de seguridad que desee configurar y después haga clic en **Administrador de roles de seguridad**.

Para acceder al administrador de roles de seguridad para una carpeta específica

1. En Symantec Management Console, abra una vista que contenga la carpeta en la cual desea establecer los permisos de seguridad.
2. En el panel izquierdo, haga clic con el botón derecho en la carpeta y después haga clic en **Seguridad**.

Propiedad de una carpeta o elemento

Puede utilizar también el Administrador de roles de seguridad para asumir la posesión de un elemento. Esto puede ser necesario si los permisos de un elemento se eliminan accidentalmente de manera que el propietario no tenga más acceso al elemento. Al asumir la posesión de un elemento, puede restablecer los permisos apropiados y restaurar el acceso al propietario original.

Para asumir la posesión de una carpeta o elemento, precisa el privilegio Asumir posesión y el permiso Control total en la carpeta o el elemento. El rol del administrador de Symantec cuenta con este privilegio y este permiso en todos los elementos y carpetas.

Ver "Personalización de permisos de herencia" en la página 104.

Para asumir la posesión de una carpeta o elemento

1. En el Administrador de roles de seguridad, en el panel izquierdo, seleccione la carpeta o el elemento para los cuales desea asumir la posesión.
2. En el panel derecho, haga clic en **Opciones avanzadas**.
3. En la ventana Permisos para: En la ventana *Artículo*, haga clic en **Asumir posesión**.
4. Haga clic en **Guardar cambios**.
5. Haga clic en **Cancelar** para cerrar la ventana Permisos para: *Nombre del elemento*.

Cómo administrar credenciales

Credential Manager proporciona una ubicación segura de almacenamiento para los nombres de usuario y las contraseñas. Las soluciones de administración instaladas definen los tipos de credenciales que Credential Manager almacena.

Ver "Categorías de permisos de seguridad" en la página 491.

Ver "Permisos de Credential Manager" en la página 509.

El acceso a las credenciales se controla mediante el sistema de seguridad incorporado basado en roles de Symantec Management Platform.

Las soluciones de administración crean típicamente credenciales cuando son necesarias para realizar una tarea. Para definir una credencial manualmente, es necesario conocer el tipo de credencial que se usa y la información necesaria para ese tipo de credencial.

Cuando se crea una credencial, solamente se concede acceso al creador. La edición de credenciales permite actualizar la contraseña y otorga acceso a usuarios y grupos adicionales.

Es posible también eliminar la credencial. Antes de eliminar una credencial, asegúrese de que no sea necesaria como parte de una tarea de administración activa.

Para crear una credencial

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Todas las configuraciones**.
2. En el panel izquierdo, haga clic en **Supervisión y alertas > Configuración de credenciales > Administración de credenciales**.
3. En el panel derecho, haga clic en **Agregar credenciales**.
4. En el cuadro de diálogo **Agregar credencial**, seleccione un tipo credencial y, después, proporcione los valores necesarios.
5. Haga clic en **Aceptar**.

Para editar una credencial

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Todas las configuraciones**.
2. En el panel izquierdo, haga clic en **Supervisión y alertas > Configuración de credenciales > Administración de credenciales**.
3. En el panel derecho, seleccione un credencial y después haga clic en **Editar**.
4. En el cuadro de diálogo **Editar credencial**, actualice la credencial y, después, haga clic en **Aceptar**.

Capítulo 5

Configuración de programaciones

En este capítulo se incluyen los temas siguientes:

- Cómo Symantec Management Platform usa las programaciones
- Componentes de una programación de Symantec Management Platform
- Cómo administrar programaciones compartidas
- Configuración de una programación
- Visualización del calendario interno de programaciones de Notification Server

Cómo Symantec Management Platform usa las programaciones

Symantec Management Platform usa programaciones para las tareas y las políticas.

Ver "Componentes de una programación de Symantec Management Platform" en la página 119.

Tabla 5-1 Usos de las programaciones

Uso	Descripción
Programación de las tareas y las políticas del servidor	Muchas operaciones de Symantec Management Platform se programan para ejecutarse en intervalos regulares. Algunas de estas operaciones necesitan ejecutarse con frecuencia. Por ejemplo, actualizar la pertenencia de los filtros y los grupos de recursos; o la depuración de registros viejos de la CMDB, pueden realizarse con menor frecuencia. Por lo general, estas programaciones se configuran para repetirse en intervalos regulares y permanecen activas por tiempo indeterminado.
Programación de tareas del agente	Las programaciones pueden usarse cuando se desea realizar una operación en un equipo administrado. Por ejemplo, distribuir un parche para reparar una vulnerabilidad en una aplicación o recopilar el inventario para el cumplimiento de alguna regla. Por lo general, se desea realizar la operación de inmediato y ejecutarla solamente una vez. Es posible programar las tareas del agente de manera que se ejecuten: ■ De forma inmediata ■ Inmediatamente, si una ventana de mantenimiento está abierta. ■ La próxima vez que un usuario inicie sesión en el equipo. ■ La próxima vez que se inicie el equipo. En algunas ocasiones es posible que el usuario desee programar la operación para que se ejecute en una fecha y una hora específicas. Por ejemplo, el próximo domingo a las 9:00 p.m., para asegurarse de que no interfiera con el trabajo del usuario. En raras ocasiones es necesario programar una tarea para que se repita. Sin embargo, una operación que se repite generalmente se considera una política basada en tareas.

Uso	Descripción
Programación de políticas del agente	Una política de agente es una declaración sobre cómo un equipo se debe administrar. Por ejemplo, una política de agente puede: ■ Impedir que se ejecute el software ■ Exigir que se instale el software ■ Exigir que la antigüedad de la información de inventario sobre un equipo no supere los N días Para funcionar correctamente, algunas políticas de agente deben ser programadas para ejecutarse en los intervalos correctos. Por ejemplo, una política de cumplimiento del software debe verificar periódicamente que el equipo cumpla con las reglas y, si no lo hace, realizar la reparación adecuada. Asimismo, una política de inventario debe asegurarse de que los datos del inventario sean actuales. Por lo general, estas programaciones son recurrentes y pueden repetirse durante el día de trabajo. Normalmente, las políticas de agente se programan para ejecutarse cuando el equipo se inicia o cuando un usuario inicia sesión. Cuando se configuran estas programaciones, también es necesario tener en cuenta cómo interactúan con las ventanas de mantenimiento configuradas en los equipos administrados. Ver "Configuración de las opciones de configuración global de agente" en la página 277. Ver "Configuración de las opciones de configuración del agente de destino" en la página 278.
Programación de las ventanas de mantenimiento del agente	La programación de una ventana de mantenimiento es esencialmente una programación recurrente que tiene una duración. No es necesario programar las ventanas de mantenimiento para el inicio del equipo, el inicio de sesión del usuario u otros eventos. No es necesario que las ventanas de mantenimiento se repitan durante el día de trabajo. Ver "Configuración de políticas de ventana de mantenimiento" en la página 280.

Componentes de una programación de Symantec Management Platform

Las programaciones de Symantec Management Platform permiten realizar operaciones repetitivas y extraordinarias en el equipo con Notification Server y los equipos administrados durante los períodos apropiados, sin intervención manual. Por ejemplo, los filtros de recurso deben actualizarse con frecuencia, la CMDB debe ser depurada regularmente y los paquetes deben actualizarse en los intervalos apropiados. Todas estas tareas se deben programar para ejecutarse en el momento y con la frecuencia que mejor se adapte a las necesidades de la organización.

Ver "Cómo Symantec Management Platform usa las programaciones" en la página 117.

Symantec Management Platform usa dos tipos de programaciones:

Compartida	Estas programaciones se definen en Notification Server como elementos compartidos que están disponibles para ser utilizados en cualquier operación programada. Ver "Cómo administrar programaciones compartidas" en la página 122.
Personalizada	Estas programaciones se configuran en forma independiente dentro de cada tarea, política o regla que se programe. No se pueden compartir con ninguna otra tarea, política o regla.

Tabla 5-2 Componentes de una programación

Componente	Descripción
Zona horaria y período activo	La zona horaria y el período activo definen el período dentro del cual se puede ejecutar una programación. Todas las programaciones, las activaciones y los modificantes tienen las propiedades siguientes: ■ **Zona horaria** La zona horaria en la cual se programa la tarea que desea ejecutarse. La zona horaria puede ser Local, Servidor o UTC. ■ **Fecha de inicio** La fecha y la hora en que el período activo de la programación comienza. Una programación no puede activarse antes de su fecha de inicio. ■ **Fecha de finalización** La fecha y la hora en que el período activo de la programación finaliza. Si la fecha de finalización no se especifica, la programación sigue siendo activa indefinidamente. Una programación no se puede activar después de su fecha de finalización. Una programación no puede ejecutarse fuera de su período activo. Esto se aplica incluso si la programación fue activada dentro de su período activo, pero un modificador impidió que se ejecutase en ese momento.

Componente	Descripción
Activaciones	Una activación es un evento que hace que se active la programación. Una activación puede ser una hora y una fecha específica, o un evento como el inicio de sesión de un usuario a un equipo. Las activaciones controlan el momento en el que se ejecuta y se repite la programación. Si una programación contiene varias activaciones, se ejecuta cada vez que una de sus activaciones se produce. Las activaciones de la programación pueden tener las propiedades siguientes: ■ Exacta Determina el comportamiento cuando una tarea programada no se puede realizar en la hora exacta en la cual está programada. Si la propiedad está configurada como verdadera, la tarea programada se ejecuta en la hora exacta o no se ejecuta. Si las condiciones son tales que la tarea no se puede realizar en la hora programada exacta, la tarea programada no se realiza. Si la propiedad está configurada como falsa, la tarea programada se ejecuta en la hora exacta o lo más pronto posible después de la hora programada. Por ejemplo, se programa la ejecución de una tarea cada noche a las 2:00 a. m., pero el equipo está siempre apagado a esa hora. La configuración exacta permite ejecutar la tarea siempre que el equipo se encienda después de la hora. Esta propiedad se aplica para el inicio de sesión, el inicio y otros eventos, así como las horas especificadas. ■ Duración La cantidad de tiempo que la programación está activa. La duración puede ser hasta 24 horas. ■ Repetición El intervalo en el cual la tarea debe repetirse durante el período activo de la programación. El intervalo de repetición puede ser hasta 24 horas.

Componente	Descripción
Modificantes	Los modificantes son las condiciones adicionales que son necesarias para que la programación se active. Todos los modificantes se aplican a todas las activaciones. ■ Sólo si hay un usuario conectado Cuando la activación ocurre en un equipo de destino, Symantec Management Agent comprueba ese equipo para asegurarse de que un usuario haya iniciado sesión antes de ejecutar la programación. Si ningún usuario ha iniciado sesión, la programación no se ejecuta en ese equipo. ■ Sólo si no hay ningún usuario conectado Cuando la activación ocurre, el equipo de destino se analiza para asegurarse de que ningún usuario haya iniciado sesión. Si un usuario ha iniciado sesión, la programación no se ejecuta en ese equipo.

Cómo administrar programaciones compartidas

Varios elementos programados (tales como políticas, tareas o reglas de replicación) pueden usar una programación compartida. La alternativa a usar una programación compartida es definir una programación personalizada dentro de la política o de la tarea.

Ver "Componentes de una programación de Symantec Management Platform" en la página 119.

Las programaciones compartidas no pueden reemplazar a las ventanas de mantenimiento. Si desea que un elemento programado se ejecute fuera de una ventana de mantenimiento, es necesario configurar la programación personalizada apropiada.

Se proporciona un conjunto de programaciones compartidas predeterminadas con Symantec Management Platform. Es posible modificarlas para que se adapten a sus requisitos, pero no se pueden eliminar. Por ejemplo, puede configurar la programación de horario de oficina para que se ejecute en intervalos regulares durante las horas de trabajo normales. Es posible configurar la programación de actualización del paquete para que se ejecute en un momento conveniente fuera de horas de trabajo. Es posible también crear cualquier nueva programación compartida que necesite y eliminarla cuando ya no sea necesaria.

Es posible habilitar o deshabilitar cada programación compartida según sea necesario. Todas las programaciones compartidas habilitadas están disponibles para cualquier elemento programado. Si deshabilita una programación compartida, se deshabilita cualquier elemento programado que use la programación.

Ver "Visualización del calendario interno de programaciones de Notification Server" en la página 124.

Para administrar programaciones compartidas

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Notification Server > Programaciones compartidas**.
2. En la página **Programaciones compartidas**, realice una de las siguientes acciones:

Para agregar una programación nueva	Haga clic en **Agregar programación** y, a continuación, en el Editor de programaciones, especifique los detalles apropiados. Ver "Configuración de una programación" en la página 123.
Para editar una programación	Haga clic en el nombre de la programación y, a continuación, en el Editor de programaciones, especifique los detalles apropiados. Ver "Configuración de una programación" en la página 123.
Para habilitar una programación	Seleccione la casilla apropiada. Si desea deshabilitar la programación, anule la selección de la casilla.
Para eliminar una programación	En el extremo derecho de la fila apropiada, haga clic en **Eliminar**.
Para ver qué elementos están utilizando una programación actualmente	En la lista desplegable **Elementos que utilizan actualmente**, seleccione la programación apropiada. Los nombres de todos los elementos (tales como tareas, políticas y reglas de replicación) que utilizan la programación seleccionada se muestran en el panel inferior.

Configuración de una programación

El **Editor de programaciones** permite configurar una programación que se adapte a sus requisitos.

Ver "Componentes de una programación de Symantec Management Platform" en la página 119.

Ver "Cómo administrar programaciones compartidas" en la página 122.

Para configurar una programación

1. En la ventana **Editor de programaciones**, en el cuadro **Nombre**, escriba el nombre de la programación.
2. En **Tarea de programación**, seleccione la frecuencia de programación o activación.
3. En la ficha **Detalles**, especifique la hora de inicio de la programación, así como los días, las semanas o los meses en los cuales desea ejecutarla.
4. Si desea que la programación permanezca activa en un intervalo determinado de fechas, en la ficha **Avanzado**, especifique las fechas de inicio y finalización apropiadas.

   Según las opciones predeterminadas, una nueva programación se activa inmediatamente después de su creación (a partir de la fecha actual). La programación permanece activa por tiempo indeterminado (no se especifica ninguna fecha de finalización).
5. Si desea que la programación repita una tarea en intervalos regulares cada vez que se ejecuta la programación, en la ficha **Avanzado**, seleccione **Repetir tarea**.

   Especifique la frecuencia y la duración apropiadas.
6. Si desea que esta programación contenga varias programaciones, seleccione **Usar varias programaciones**.
7. Cada vez que desee agregar una programación adicional a esta programación, haga clic en **Nueva** y complete los pasos 2 a 5.
8. Haga clic en **Aceptar**.

Visualización del calendario interno de programaciones de Notification Server

Es posible ver la información de programaciones de Notification Server en el calendario interno de programaciones de Notification Server. Los elementos programados que puede ver en el Calendario incluyen las tareas que se ejecutan en Notification Server, las políticas y las políticas de automatización. Además, incluyen programaciones compartidas, períodos de bloqueo, ventanas de mantenimiento y programaciones internas de Notification Server. Las soluciones de Symantec pueden incorporar elementos programados adicionales al calendario.

Ver "Componentes de una programación de Symantec Management Platform" en la página 119.

Los siguientes tipos de elementos programados se visualizan:

Elementos del período	Definen solamente una hora de inicio y se ejecutan por un período indefinido. Los ejemplos incluyen las ventanas de mantenimiento, los períodos de bloqueo y las programaciones compartidas.
Elementos de eventos	Tienen una hora de finalización definida. Los ejemplos incluyen tareas, trabajos, programaciones personalizadas y políticas. Tenga en cuenta que las políticas no siempre se ejecutan en las horas que se muestran en el calendario. Las políticas no son tan deterministas como las tareas, de forma que pueden estar sujetas a retrasos. Las tareas y los trabajos se ejecutan siempre en las horas que se muestran en el calendario.

La vista Calendario permite ver qué programaciones se configuran por períodos determinados, tales como días, semanas o meses específicos. En la vista Semana y la vista Mes, se puede hacer clic en un día determinado para abrir la vista Día para ese día.

Algunos elementos programados usan programaciones compartidas, en lugar de definir sus propias programaciones. Las relaciones de programación compartida se representan en el panel izquierdo de la vista Día. Los elementos programados se agrupan en programación compartida a la cual se refieren.

Cada programación tiene un símbolo asociado que lo vincula a la página de configuración apropiada, si está disponible. Es posible hacer clic en el símbolo para examinar la página de configuración, que se abre en una ventana nueva. Si ninguna página de configuración está disponible para una programación, se usa el símbolo predeterminado del calendario y no existe ninguna función de examen de niveles inferiores.

Ver "Cómo administrar programaciones compartidas" en la página 122.

Ver "Configuración de una programación" en la página 123.

Para ver el calendario de programaciones de Notification Server

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Todas las configuraciones**.
2. En el panel izquierdo, expanda **Configuración > Notification Server** y, a continuación, haga clic en **Calendario de programación interna**.
3. En la página **Vista del calendario para las programaciones internas de NS**, en la lista desplegable **Ver**, seleccione la vista que desea usar.

4 Seleccione el período que desee ver al hacer clic en el símbolo apropiado:

Día	Muestra los detalles de cada programación que se ejecuta una o más veces por día. Las programaciones se enumeran de acuerdo con sus horas de inicio. El panel izquierdo enumera las programaciones y el panel derecho muestra sus incidencias en el calendario. La vista Día es la vista predeterminada. Cada incidencia de un elemento del período se visualiza como un diamante. Cada incidencia de un elemento del evento se visualiza normalmente como una barra, pero las que ocurren con intervalos muy cortos se visualizan como pequeños diamantes. Para obtener claridad en la pantalla, los eventos con un intervalo menor de 15 minutos (de forma predeterminada) se omiten. El color en segundo plano identifica las horas de oficina que se definen para la organización.
Semana	Muestra los detalles de cada programación que se ejecuta menos de una vez por día; pero, por lo menos, una vez por semana.
Mes	Muestra los detalles de cada programación que se ejecuta menos de una vez por semana. Se omiten los elementos del período y los elementos de eventos se resumen a sus horas de inicio, horas de finalización y títulos.

5 Para ver períodos anteriores o posteriores, haga clic en **Anterior** o **Después**, cualquiera es apropiado.

Capítulo 6

Configurar los sitios y los servidores de sitio

En este capítulo se incluyen los temas siguientes:

- Acerca de los servicios de sitio
- Acerca del mantenimiento del sitio
- Administración de sitios
- Administración de servidores de sitio
- Cómo asignar un servidor de sitio a un sitio de forma manual
- Cómo administrar agentes asignados de forma manual
- Administración de subredes
- Acerca de la configuración del servicio de sitio
- Configuración de Package Service
- Cómo establecer la configuración del servicio de tareas

Acerca de los servicios de sitio

Symantec Management Platform puede albergar varios tipos de componentes de software intermedio, como servidores de paquetes, Task Server y servidores de arranque. Los componentes de software intermedio se pueden instalar en cualquier equipo, a excepción de los equipos con Notification Server. Estos servicios actúan como el primer punto del contacto para Symantec Management Agents, lo que reduce la carga en Notification Server.

El nombre oficial para un componente de software intermedio es “servicio de sitio.” Cualquier equipo que albergue un servicio de sitio es conocido como servidor de sitio. Un servidor de sitio puede tener uno o más servicios de sitio instalados en él. Por ejemplo, si se instala el servicio de sitio del servidor de paquetes (el “servicio de paquetes”) en un equipo, ese equipo se convierte en servidor de sitio.

Los servidores de sitio pueden ayudar a Notification Server. Los servidores de sitio pueden ampliar la arquitectura, mejorar la eficacia de distribución y disminuir los requisitos de ancho de banda de red.

Notification Server controla el despliegue, la configuración y el mantenimiento continuo de los servicios de sitio. El servicio de administración de paquetes, el servicio de tareas y el servicio del inicio proporcionan Symantec Management Agents con paquetes, tareas y difusiones PXE.

Notification Server realiza las siguientes funciones para la administración del sitio:

- Controla la implementación y la eliminación de los servicios de sitio a los servidores de sitio y desde ellos
- Garantiza que el servicio de sitio esté instalado solamente en los equipos que cumplen con los requisitos mínimos del sistema

Se usa mantenimiento del sitio para crear grupos lógicos de endpoints para equilibrar la carga en los servidores de sitio. Por ejemplo, puede distribuir paquetes eficientemente a sus Symantec Management Agents con varios servidores de paquetes. Los servidores de paquetes controlan la mayoría de las funciones de distribución de paquetes, lo que libera a Notification Server de realizar otras actividades.

Ver "Acerca del mantenimiento del sitio" en la página 128.

Acerca del mantenimiento del sitio

El mantenimiento del sitio es la administración de sitios, subredes y servicios de sitio de la organización. Es posible administrar los equipos según el sitio y la subred, lo que permite controlar los grupos de equipos mientras se minimiza el consumo de ancho de banda. Un sitio es, por lo general, una ubicación física de la organización (por ejemplo, un edificio determinado o un piso de un edificio). Una subred es un intervalo de direcciones lógicas de la red.

En condiciones de funcionamiento normales, cada servidor de paquetes o Task Server brinda servicio solo a los Symantec Management Agents que existen dentro de los sitios asignados. Si no se ha definido ningún sitio, todos los servidores de sitio quedan disponibles para dar servicio a todos los equipos con Symantec Management Agents (aunque este método no se recomienda).

Si no se define ningún sitio para un servidor de paquetes o un Task Server, Notification Server usa las reglas siguientes:

- Notification Server primero intenta encontrar cualquier servidor de sitio en la misma subred que el equipo solicitante. Si se encuentra alguno, estos servidores de sitio se vuelven a los equipos con Symantec Management Agent.
- Si no se encuentra ningún servidor de sitio en la misma subred del equipo solicitante, todos los servidores de sitio se vuelven a Symantec Management Agent.
- Si ningún servidor de sitio está disponible, el agente se dirige al equipo con Notification Server.

El usuario puede asignar servidores de sitio a los sitios mediante los siguientes métodos:

- Asigne la subred que contiene el servidor de sitio a un sitio.
  Ver "Administración de subredes" en la página 135.
- Asigne el servidor de sitio a un sitio.
  Ver "Cómo asignar un servidor de sitio a un sitio de forma manual" en la página 133.
- Utilizar Connector para Active Directory para que realice la tarea.
  Connector para Active Directory anula las subredes y los sitios que están en conflicto con él. Por ejemplo, si se asignan manualmente subredes a un sitio que está en conflicto con el contenido de Connector para Active Directory, se usa la información de Active Directory.

Una vez que la lista de servidores de sitios disponibles se vuelva a Symantec Management Agent, el agente elegirá el servidor de sitio más conveniente.

Los servidores de sitio y los equipos administrados pueden tener varios NIC y direcciones IP; por lo tanto, pueden pertenecer a más de un sitio por medio de la asignación de subred.

Ver "Acerca de los servicios de sitio" en la página 127.

Ver "Administración de sitios" en la página 129.

Ver "Administración de servidores de sitio" en la página 131.

Ver "Administración de subredes" en la página 135.

Administración de sitios

Es necesario configurar todos los sitios necesarios en su organización. Es posible ejecutar una regla de importación del sitio a fin de recopilar automáticamente la información del sitio para la organización desde Active Directory. También se

pueden crear sitios manualmente y asignarles los servidores de sitio y las subredes adecuadas.

Para administrar sitios

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Notification Server > Configuración del Servidor de sitio**.
2. Efectúe uno de los pasos siguientes:

Crear un nuevo sitio	1. En el panel izquierdo, haga clic en **Nuevo > Sitio**. 2. En el cuadro **Nombre** de la ventana **Nuevo sitio**, escriba el nombre del nuevo sitio. 3. Si desea asignar subredes al sitio de forma inmediata, especifique las subredes apropiadas. 4. Haga clic en **Aceptar**.
Modificar un sitio	1. En el panel izquierdo, seleccione el sitio que desee modificar y, después, haga clic en **Configurar**. 2. Si desea cambiar el nombre del sitio, en el cuadro **Nombre** de la ventana **Editar sitio**, escriba el nuevo nombre. 3. Para cambiar las subredes que son asignadas al sitio, especifique las subredes apropiadas. 4. Haga clic en **Aceptar**.
Eliminar un sitio	En el panel izquierdo, seleccione el sitio que desee eliminar y, después, haga clic en **Eliminar**. Las subredes que se asignan al sitio no se eliminan. Su estado pasa a ser sin asignar y se los puede asignar a un sitio diferente. Los servidores de sitio de las subredes afectadas no se usan hasta que se asignen a un sitio diferente.
Eliminar manualmente un servidor de sitio asignado desde un sitio	En el panel izquierdo, en el servidor de sitio, seleccione el sitio que desee quitar y, a continuación, haga clic en **Eliminar**. El servidor de sitio no está afectado y continúa funcionando como servidor para cualquier otro sitio al cual esté asignado. Esta opción se aplica solamente a los servidores de sitio que se asignan manualmente a los sitios. No se puede quitar de un sitio un servidor de sitio que está conectado a un sitio mediante una subred.

Eliminar una subred de un sitio	En el panel izquierdo, en el sitio, seleccione la subred que desee eliminar y, después, haga clic en **Eliminar**. Si se elimina una subred, no queda asignada a ningún sitio. Las subredes incluidas que no se asignan manualmente a un sitio también quedan sin asignar. Los servidores de sitio de la subred o las subredes incluidas ya no dan servicio al sitio. Sin embargo, continúan dando servicio a los sitios a los cuales fueron asignados manualmente.
Administrar agentes asignados de forma manual	Es posible asignar agentes a un sitio y eliminar cualquiera que ya no necesite. Ver "Cómo administrar agentes asignados de forma manual" en la página 134.

Administración de servidores de sitio

Es necesario crear todos los servidores de sitio que se necesitan en su organización y asignarlos a los sitios apropiados. Para crear los servidores de sitio, seleccione los equipos que desee usar y especifique los servicios de sitio que desee instalar en cada uno. También se pueden modificar los servidores de sitio existentes al agregar o quitar servicios de sitio. Notification Server implementa los paquetes de instalación apropiados a los equipos seleccionados y elimina los que ya no se necesitan. Tenga en cuenta que los cambios se aplican cuando los equipos de destino con Symantec Management Agents solicitan la siguiente configuración, de modo que es posible que no se implementen de forma inmediata.

Para asegurarse de que los servicios de sitio se instalen y se configuren correctamente, Symantec recomienda que se instalen los servicios de sitio con Symantec Management Console.

Nota: El equipo con Task Server debe tener las funciones de IIS 6.0 o IIS 7.0 y .NET Framework 3.5 habilitadas.

Cuando se selecciona un servidor de sitio, la página Servicios de sitio muestra las estadísticas de cada servicio de sitio instalado en él. La vista contraída muestra los detalles del resumen, y la vista expandida abre un panel para cada servicio de sitio que muestra todos los detalles y la información gráfica. Cada panel de servicio del sitio también incluye un vínculo a la página de configuración global correspondiente.

La barra de título de cada servicio del sitio contiene un símbolo que muestra su estado actual:

Verde	El servicio está instalado y en ejecución en el servidor de sitio.
Amarillo	El servicio no está instalado actualmente en el servidor de sitio.
Naranja	El servicio está en estado de advertencia.
Rojo	El servicio no puede utilizarse. Un paquete es no válido.

Para administrar los servidores de sitio

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Notification Server> Configuración del Servidor de sitio**.
2. Efectúe uno de los pasos siguientes:

Crear un servidor de sitio	1. En el panel izquierdo, haga clic en **Nuevo > Servidor de sitio**. 2. En la ventana **Seleccionar equipos**, seleccione los equipos a los cuales desee agregar los servicios de sitio y haga clic en **Aceptar**. La lista que se encuentra en el panel izquierdo contiene todos los equipos que están disponibles para usarse como servidores de sitio. Cuando se instala Symantec Management Platform, es necesario dar unos minutos al sistema para que rellene la lista. 3. En el cuadro de diálogo **Agregar o quitar servicios**, seleccione las casillas apropiadas para seleccionar los servicios de sitio que desee instalar en cada servidor de sitio y haga clic en **Siguiente**. Todos los servicios de sitio disponibles aparecen debajo de cada equipo, lo que permite que se seleccione cualquier combinación de servicios para cada equipo. Las casillas de verificación de los tipos de servicios que no pueden instalarse en un equipo determinado aparecen en color gris. Es posible agrupar la lista por servidores de sitio o por servicios. Si se selecciona un nodo principal en la lista, se seleccionan todos sus servidores secundarios. Si alguna casilla de verificación ya está seleccionada, significa que el servicio de sitio correspondiente ya se encuentra instalado. Si desea quitarla, anule la selección de la casilla de verificación. 4. Haga clic en **Aceptar**.

Modificar un servidor de sitio	1 En la tabla **Información detallada**, asegúrese de que la vista Servidores de sitio esté seleccionada y, a continuación, seleccione el servidor de sitio adecuado. 2 Haga clic en el símbolo **Editar**.
Asigne un servidor de sitio de forma manual a un sitio	Seleccione el servidor de sitio apropiado y, después, haga clic en **Asignar a sitio**. Ver "Cómo asignar un servidor de sitio a un sitio de forma manual" en la página 133.
Eliminar manualmente un servidor de sitio asignado desde un sitio	En el panel izquierdo, en el servidor de sitio, seleccione el sitio que desee quitar y, a continuación, haga clic en **Eliminar**. El servidor de sitio no está afectado y continúa funcionando como servidor para cualquier otro sitio al cual esté asignado. Esta opción se aplica solamente a los servidores de sitio que se asignan manualmente a los sitios. No se puede quitar de un sitio un servidor de sitio que está conectado a un sitio mediante una subred.

Video: para obtener más información acerca de iniciar un Task Server, vea Rolling out a Task Server with ITMS Video - Part 1, Windows XP (Cómo iniciar un Task Server con ITMS, Parte 1, para Windows XP) y Rolling out a Task Server with ITMS Video - Part 2, Windows 2008 R2 (Cómo iniciar un Task Server con ITMS, Parte 2, para Windows 2008 R2) en Symantec Connect.

Cómo asignar un servidor de sitio a un sitio de forma manual

Los servidores de sitio dan servicio automáticamente al sitio al que está asignada la subred principal. Los servidores de sitio pueden tener varios NIC/IP y estar en más de una subred, de forma que pueden pertenecer a más de un sitio. El usuario también puede asignar manualmente cada servidor de sitio a uno o más sitios. La columna Asignados de forma manual de la tabla Información detallada indica si el servidor de sitio fue asignado manualmente al sitio.

Ver "Administración de servidores de sitio" en la página 131.

Cuando se asigna manualmente un servidor de sitio a un sitio, solamente se asigna el servidor de sitio al sitio seleccionado. La subred a la cual pertenece el servidor de sitio no se ve afectada.

Para asignar un servidor de sitio a un sitio de forma manual

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Notification Server> Configuración del Servidor de sitio**.
2. En la tabla **Información detallada**, asegúrese de que la vista Servidor de sitio esté seleccionada y, a continuación, seleccione los servidores de sitio adecuados.
3. Haga clic en **Asignar a sitio**.
4. En la ventana **Seleccionar un sitio**, seleccione el sitio al cual desee asignar el servidor de sitio.
5. Haga clic en **Aceptar**.

Cómo administrar agentes asignados de forma manual

Un agente asignado de forma manual es un equipo que se ha asignado manualmente a un sitio en lugar de asignarlo a través de la subred. Es posible asignar manualmente equipos determinados a un sitio para separarse de la asignación de la subred. Es posible asignar manualmente nuevos agentes a un sitio asignando los recursos de destino relevantes al sitio. Es posible quitar cualquier agente que no desee del sitio asignando los destinos de recurso apropiados a un sitio diferente.

Nota: Cuando el agente asignado manualmente es Task Server, el cambio no se formaliza, a menos que se restablezca Symantec Management Agent en el equipo. Una manera de restablecer Symantec Management Agent es hacer clic en **Restablecer el agente** en la ficha **Estado de tarea** en Symantec Management Agent. Otra manera es ejecutar la tarea de restablecer el agente de tareas en el equipo.

Para administrar agentes asignados de forma manual

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Notification Server> Configuración del Servidor de sitio**.
2. En el panel izquierdo, expanda el sitio o el servidor de sitio que desee modificar y después haga clic en **Agentes asignados de forma manual**.
3. En la página **Agentes asignados de forma manual**, realice una de las siguientes acciones:

Agregar agentes asignados de forma manual a un sitio	Haga clic en **Nuevo** y, a continuación, en la ventana **Seleccione un grupo**, seleccione o cree los destinos de recurso apropiados. Ver "Cómo seleccionar los destinos de recursos con nombre" en la página 386.
Reasignar agentes asignados de forma manual a otro sitio	Esta opción está disponible solamente en el nodo de sitio, no en el nodo de servicios de sitio. Seleccione los destinos de recursos apropiados y después haga clic en **Asignar a sitio**. En la ventana **Seleccionar un sitio**, seleccione el sitio apropiado y después haga clic en **Aceptar**.
Eliminar los agentes asignados de forma manual de un sitio	Seleccione los destinos de recursos apropiados y después haga clic en **Eliminar**.

Administración de subredes

Es necesario crear todas las subredes de su organización y asignarlas a los sitios apropiados. Se pueden volver a sincronizar las subredes cuando sea necesario y eliminar cualquier subred que ya no exista.

Las subredes pueden ser determinadas de los datos del inventario básico que se importan de Active Directory o se agregan manualmente. Es posible ejecutar una

regla de importación de subredes para recopilar automáticamente la información de la subred de Active Directory.

Las subredes se añaden como sufijo siempre con el número de bits establecido en la máscara de red, por ejemplo, 192.168.0.0/24. Las subredes siempre se visualizan en un árbol jerárquico. Se aplica el ámbito del recurso, de forma que solamente se pueden ver las subredes que contienen los recursos a los cuales se tiene acceso.

Es necesario asignar cada subred al sitio apropiado. De forma predeterminada, las subredes incluidas (subredes cuyo intervalo IP está completamente incluido en otra subred) se asignan automáticamente al mismo sitio. Sin embargo, la inclusión de subredes se puede anular manualmente asignando de forma explícita una subred incluida a un sitio diferente. De forma predeterminada, las subredes incluidas se visualizan en el panel izquierdo, debajo de las subredes principales. Sin embargo, cuando una subred incluida se asigna manualmente a un sitio diferente de su red principal, se visualiza debajo del sitio al cual está asignada

Los servidores de sitio de una subred se asignan automáticamente al mismo sitio que la subred. Esta asignación no se daña si se asigna manualmente un servidor de sitio a un sitio diferente. Un servidor de sitio se puede asignar manualmente a cualquier cantidad de sitios, además del sitio al que da servicio mediante la asignación de subred.

Para administrar subredes

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Notification Server > Configuración del Servidor de sitio**.
2. Efectúe uno de los pasos siguientes:

Crear una subred nueva

1. En el panel izquierdo, haga clic en **Nuevo > Subred**.
2. En el cuadro de diálogo **Subred nueva**, especifique la dirección de red de la subred, la máscara de subred, el sitio a quien desee asignar esta subred y después haga clic en **Aceptar**.

   Cuando se presiona la tecla **Tab** o se hace clic en este cuadro después de establecer la dirección de red de la subred, automáticamente se selecciona una máscara según las reglas siguientes:

   - El sistema examina el primer octeto de una dirección IPv4 para determinar si es una subred de clase A, B o C. A continuación, selecciona la máscara predeterminada apropiada.
   - Si la dirección de red es más específica (es decir, tiene más octetos sin ceros) de lo permitido para esa clase, los bytes adicionales se establecen en la máscara predeterminada.
   - Si la dirección no tiene un formato reconocido, o el último octeto no es cero, no se sugiere la máscara predeterminada.

   Si es necesario, la máscara predeterminada se puede editar de forma manual. Tenga en cuenta que una vez que se edita manualmente la máscara de subred, la actualización de la dirección de red en el cuadro **Subred** ya no actualiza la máscara.

Eliminar una subred

En el panel izquierdo, expanda **Administración del sitio > Subredes**, seleccione la subred que desee eliminar y después haga clic en **Supr**.

Si se elimina una subred creada manualmente, se elimina de forma permanente. Sin embargo, las subredes importadas desde el inventario básico o Active Directory se restauran cuando se actualizan los datos.

Asignar una subred a un sitio

1. En el panel izquierdo, expanda **Administración del sitio** y después haga clic en **Subredes**.
2. En el panel derecho, seleccione la subred correspondiente y, luego, haga clic en **Asignar a sitio**.
3. En el cuadro de diálogo **Seleccionar un sitio**, seleccione el sitio al cual desee asignar la subred y después haga clic en **Aceptar**.

Volver a sincronizar las subredes	1 En el panel izquierdo, expanda **Administración del sitio** y después haga clic en **Subredes**. 2 En el panel derecho, haga clic en **Volver a sincronizar subredes**. Notification Server consulta la información actual de la subred en la CMDB. Lee la asignación de subred incluida en los resultados del último análisis de Inventario del agente. Entonces Notification Server actualiza la lista de subredes según corresponda.

Acerca de la configuración del servicio de sitio

La configuración del servicio de sitio es generalmente una configuración predeterminada global. Cualquier cambio que se realice en la configuración de un tipo de servicio de sitio determinado se aplica a todos los servicios de sitio de ese tipo. Sin embargo, algunos tipos de servicio de sitio pueden tener una configuración que se define en servicios individuales y anula así los valores predeterminados globales. Por ejemplo, los servidores de paquetes se pueden configurar como Restringidos o Sin restricciones y anular así la configuración predeterminada.

Es posible ver y modificar la configuración global de cada servicio de sitio. Cada servicio de sitio, como los servidores de paquetes, tiene una página que permite editar su configuración global.

En el panel izquierdo, se muestra cada servicio instalado debajo de cada servidor de sitio. La página correspondiente muestra el resumen del servicio para el servidor de sitio. El panel se expande de forma predeterminada, en lugar de contraerse, para mostrar las estadísticas como en la página Servidor de sitio. El vínculo Cambiar configuración permite editar la configuración global de ese tipo de servicio.

Para muchos servicios, la información de resumen que se muestra aquí puede ser igual que la información de resumen que se puede expandir en la página Servidor de sitio. Sin embargo, Symantec Management Platform permite que un servicio proporcione un control diferente en este contexto, si es apropiado. Por ejemplo, si hay una página completa de datos disponible, se visualiza en la página Servicio de sitio. Se visualiza un conjunto de datos condensado en la página Servidor de sitio.

Ver "Configuración de Package Service" en la página 139.

Ver "Cómo establecer la configuración del servicio de tareas" en la página 139.

Consulte los temas sobre el servicio de supervisión en la *Guía del usuario de Monitor Solution*.

Configuración de Package Service

Es necesario definir la configuración global de Package Service. Esta configuración se aplica a todos los Package Services que están instalados en los servidores de sitio de la Plataforma de administración Symantec.

Para configurar Package Service

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Notification Server> Configuración del Servidor de sitio**.
2. En el panel izquierdo, expanda **Configuración > Servicio de administración de paquetes** y después haga clic en **Configuración de Package Service**.
3. En la página **Configuración de Package Service**, establezca la configuración apropiada.

Para definir la configuración global de Package Service	En el panel **Configuración global de Package Service**, realice los cambios necesarios. Para obtener más información, haga clic en la página y después presione **F1**.
Para configurar Package Servers sin restricciones	En el panel **Selección de Package Server restringido**, configure cada Package Server. Para ello, seleccione o anule la selección de la casilla Restringidos, según sea necesario. Es posible usar la lista desplegable Sitio para ver la información de resumen sobre todos los Package Servers de un sitio específico o de todos los sitios.

4. Haga clic en **Guardar cambios**.

Cómo establecer la configuración del servicio de tareas

Es posible aplicar la configuración de Task Service a los Task Servers que usan los equipos, los usuarios o los recursos. Notification Server aplica esta configuración a los Task Services elegidos que están instalados en los servidores de sitio del entorno.

Ver "Acerca de la administración de tareas " en la página 407.

Ver "Secuenciación de tareas" en la página 416.

Para establecer la configuración del servicio de tareas

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Notification Server> Configuración del Servidor de sitio**.
2. En el panel izquierdo, expanda **Configuración > Servicio de tareas > Configuración** y después haga clic en **Configuración del Servicio de tareas**.
3. En la página **Configuración del Servicio de tareas**, establezca la configuración apropiada.

   Para obtener más información, haga clic en la página y después presione **F1**.
4. En el panel **Aplicado a**, haga clic en **Se aplica a** para seleccionar los equipos, los usuarios o los recursos a los cuales se aplica esta configuración del servicio de tareas.

   Ver "Especificación de destinos de una política o tarea" en la página 379.

   Esta configuración se aplica a los servicios de tareas que usan estos equipos, usuarios o recursos.
5. Haga clic en **Guardar cambios**.

Capítulo 7

Configuración de Package Server para Linux

En este capítulo se incluyen los temas siguientes:

- Acerca de Package Server para Linux
- Acerca de integrar al servidor web Apache con Package Server para Linux
- Acerca de detectar el servidor web Apache
- Requisitos para configurar Package Server y el servidor web Apache
- Requisitos para configurar HTTPS y HTTP
- Ejemplo de configuración de Package Server que usa el directorio web principal para los vínculos de Package Server
- Ejemplo de la configuración de Package Server usando un alias para los vínculos de Package Server

Acerca de Package Server para Linux

Para designar un equipo Linux como Package Server, asegúrese de que el equipo esté ejecutando el software siguiente:

- Symantec Management Agent para UNIX, Linux y Mac
  Este agente era previamente conocido como Altiris Agent para UNIX y Linux. Symantec Management Agent para UNIX, Linux y Mac se ejecuta en un equipo administrado. Ese agente debe coincidir con la versión del agente que está instalado en el equipo con Notification Server en Symantec Management Platform. Si el agente en el equipo administrado es anterior al agente en Notification Server, actualícelo. Una vez que el agente se actualiza, el equipo administrado puede convertirse en un Package Server.

- Versión 2.0 o 2.2 del servidor web Apache
  Ver "Acerca de integrar al servidor web Apache con Package Server para Linux" en la página 142.

Se admiten las plataformas de servidor siguientes:

- Red Hat Enterprise Linux Server 5
- Red Hat Enterprise Linux Server 6
- SUSE Linux Enterprise Server 10
- SUSE Linux Enterprise Server 11 SP1, 11 SP2

Package Server para Linux admite las ubicaciones de descarga alternativas. Las rutas para las ubicaciones alternativas son convertidas de forma automática del estilo de Windows al estilo de UNIX si se incluye la barra diagonal al final. Por ejemplo, si tiene Patch Management Solution instalado, se puede cambiar la configuración la política y del paquete al iniciar parches. En Symantec Management Console, en **Configuración > Todas las configuraciones > Software > Administración de parches**, se haga clic en una página de la configuración del distribuidor; por ejemplo, se haría clic en **Configuración de Red Hat > Configuración de reparación de parches de Red Hat**. Cuando se hace clic en la ficha **Configuración de política y paquete**, se ve la página **Configuración de reparación** para el producto seleccionado. Aquí es donde se puede seleccionar **Usar la dirección alternativa de descarga en Package Server**. Cuando se entra en la ubicación alternativa de descarga, es necesario usar la ruta completa de Windows. En esta instancia y en otras similares, incluya una barra diagonal al final de la ruta del estilo de Windows para asegurarse de que se convierta correctamente a una ruta del estilo UNIX.

Correcta: C:\path\	La barra diagonal al final significa que la ruta de Windows está convertida correctamente a /path/.
Incorrecta: C:\path\	Si omite la barra diagonal al final, la ruta de Windows se convierte incorrectamente.

Acerca de integrar al servidor web Apache con Package Server para Linux

Se integra al Package Server para Linux con el servidor web Apache para exponer los paquetes y las instantáneas de paquete a Symantec Management Agent. Las instantáneas se descargan de Notification Server a Symantec Management Agent en todas las plataformas admitidas a través de las URL HTTP.

Ver "Acerca de Package Server para Linux" en la página 141.

Los paquetes y las instantáneas de paquete se descargan en los directorios de Package Server. Los únicos archivos que se crean en el servidor web Apache son directorios, vínculos simbólicos y archivos .htaccess. Los vínculos simbólicos se crean en los archivos de paquete y los archivos de instantáneas. Los archivos .htaccess protegen los archivos de paquete con contraseñas.

Cuando un equipo Linux se convierte en un Package Server, el agente en ese equipo intenta crear dos recursos compartidos HTTP principales.

Se crean estos recursos compartidos en el espacio web virtual del servidor web Apache, de la siguiente manera:

- /Altiris/PS/Snapshots
- /Altiris/PS/Packages Nota /Altiris/PS
  Este segundo directorio se crea si es necesario.

El archivo de manifiesto del paquete no se usa cuando un Package Server para Linux descarga un paquete para la distribución. La excepción es si el paquete se encuentra en el mismo directorio para el Package Server para Linux y la entrega de software. Se configuran todos los permisos del archivo de paquete para permitir el acceso de clientes del servidor web Apache. Este acceso es típicamente a través de 0x744.

Dependiendo de la configuración específica del servidor web Apache, los directorios se crean en la raíz del directorio web. Un ejemplo es /var/www/html en un sistema típico de Linux Red Hat. Package Server Agent lee el archivo de configuración del servidor web Apache para determinar esta ubicación.

Ver "Acerca de detectar el servidor web Apache" en la página 143.

Si lo elige, puede especificar que Package Server cree los directorios en una ubicación alternativa. Use una instrucción de alias del servidor web Apache para especificar un directorio aparte.

Ver "Requisitos para configurar Package Server y el servidor web Apache" en la página 145.

Ver "Requisitos para configurar HTTPS y HTTP" en la página 146.

Acerca de detectar el servidor web Apache

Es posible detectar el servidor web Apache de forma automática o manualmente.

Ver "Acerca de integrar al servidor web Apache con Package Server para Linux" en la página 142.

Ver "Requisitos para configurar Package Server y el servidor web Apache" en la página 145.

Si elige la detección Automática, Symantec Management Agent busca el archivo ejecutable HTTPD o HTTPD2 de Apache en las ubicaciones siguientes del directorio:

- /bin:/usr/bin:/sbin:/usr/sbin:/usr/lbin:/usr/etc:/etc:/usr/bsd:/usr/local/bin:/usr/contrib/bin/
- Variable de ruta del sistema
- /opt/apache/bin:/usr/apache/bin:/usr/apache2/bin:/usr/local/apache/bin:/usr/local/apache2/bin:/usr/local/bin:/opt/freeware/apache/bin:/opt/freeware/apache2/bin:/opt/freeware/apache/sbin:/opt/hpws/apache/bin:/opt/apache2:/usr/local/apache+php

Si se encuentran los archivos ejecutables HTTPD y HTTPD2, Apache 2.0 y Apache 2.2 están instalados.

Además, si se encuentran ambos archivos ejecutables, el archivo que coincide con un proceso en ejecución se usa. El archivo predeterminado es HTTPD2.

Si el servidor web Apache no puede ser detectado de forma automática, es posible que sea necesario detectarlo manualmente. Es posible que el servidor web Apache no sea detectado de forma automática si se cambia el nombre del archivo ejecutable. Si han ocurrido varias instalaciones, el servidor web Apache incorrecto podría ser detectado. En ninguna de estas situaciones, es necesario especificar la ubicación del servidor web Apache manualmente.

Para especificar el servidor web Apache es necesario editar manualmente la sección **[httpd Integration]** del archivo client.conf en el agente. En esta sección, es necesario especificar la configuración “apache_exe_location”.

Cuando el archivo ejecutable del servidor web Apache se encuentra, se usa para determinar la ubicación predeterminada del archivo de configuración del servidor web Apache. El archivo de configuración es necesario para determinar si la instalación del servidor web Apache es conveniente para el uso de Package Server. El archivo de configuración además permite que el programa de instalación determine la configuración que es aplicable a Package Server. La configuración aplicable incluye los puertos que se usan o si el servidor está habilitado para SSL.

Si Symantec Management Agent para UNIX, Linux y Mac no puede encontrar el archivo de configuración del servidor web Apache, busca en las ubicaciones siguientes:

- /etc/httpd/conf
- /etc/httpd/2.0/conf

Como una alternativa a la detección automática se puede editar la sección **[Httpd Integration]** del archivo client.conf de Symantec Management Agent para UNIX, Linux y Mac. Cuando edite el archivo, especifique apache_config_location. Cualquier configuración que usted cambie convierte la opción en predeterminada.

Es posible usar la opción del servidor web Apache "- f" durante la instalación para volver a colocar el archivo de configuración de su ubicación predeterminada. Si vuelve a colocar el archivo, deberá especificar la ubicación de apache_config_location. Package Server para Linux no admite los archivos httpd.conf generados por mod_perl.

Requisitos para configurar Package Server y el servidor web Apache

Para que Package Server para Linux funcione con el servidor web Apache, ciertos requisitos deben ser cumplidos. Cuando se cumplen estos requisitos, Symantec Management Agent para UNIX, Linux y Mac envían el rol del servidor HTTP de Apache. Este rol permite que el equipo sea usado como Package Server para Linux.

Ver "Acerca de detectar el servidor web Apache" en la página 143.

Los requisitos de configuración son los siguientes

- La versión 2.0 o 2.2 del servidor web Apache está instalada.
- Package Server para Linux usa solamente el servidor web Apache principal o el servidor web Apache predeterminado.
  El resto de las secciones del host virtual en la configuración del servidor web Apache se omiten, con las excepciones siguientes:
  - La configuración global y el host virtual **_default_** se leen para la configuración del servidor principal.
  - Se considera al primer host virtual que define un servidor SSL el servidor SSL principal. Su configuración se usa para integrar y se omite el resto de los host virtuales SSL.
- La ubicación del espacio web del servidor web Apache donde serán creados los archivos y los directorios de Package Server debe tener las siguientes opciones habilitadas:
  - **FollowSymLinks**
  - **AllowOverride**

La ubicación del espacio web del servidor web Apache debe además ser accesible a través de HTTP anónimo. La ubicación es el directorio virtual **/Altiris/PS/**.

Ver "Requisitos para configurar HTTPS y HTTP" en la página 146.

- Si HTTP y HTTPS se definen para el servidor web Apache, se usa el servidor HTTPS.
- Se detectan y se usan los puertos no estándar, pero el servidor web Apache principal debe ser accesible a través del nombre del host del equipo. La instrucción **Escuchar** para el servidor principal debe venir antes del resto de las instrucciones **Puerto** y las políticas Escuchar en el archivo de configuración.
- El servidor web Apache debe estar en ejecución.
- No se usan módulos de compresión con el servidor web Apache. Este requisito existe porque la Entrega de paquetes no admite esos módulos.
- Es posible que sea necesario reiniciar Symantec Management Agent para UNIX, Linux y Mac una vez que se realizan cambios al archivo httpd.conf. Es posible que los archivos no surtan efecto hasta después de que se reinicie el agente.

Requisitos para configurar HTTPS y HTTP

Symantec Management Agent para UNIX, Linux y Mac usa cualquier tipo de servidor web Apache que está disponible. Puede usar HTTP o HTTPS.

Ver "Requisitos para configurar Package Server y el servidor web Apache" en la página 145.

Si el servidor web Apache admite ambos tipos de servidor web, Package Server para Linux usa HTTPS. La integración con SSL mediante HTTPS es la opción predeterminada porque es la más segura. Si desea usar el servidor HTTP, se puede cambiar la configuración **[httpd Integration] "integrate_with"**.

Tabla 7-1 Enfoques recomendados para instalar el servidor web Apache en los servidores de paquetes de soporte para UNIX y Linux

Opción	Descripción
Instale una versión con paquete del servidor web Apache. En Linux, el servidor web Apache distribuido es el más conveniente.	Esta instalación contiene los archivos ejecutables y los archivos exe del soporte técnico en **/usr/sbin** o **/usr/bin**.

Opción	Descripción
Instale el paquete del servidor web Apache en la ubicación recomendada.	Un ejemplo de una ubicación predeterminada conveniente es **/usr/local o /opt**.
Deje el directorio Configuración en su ubicación predeterminada. Este requisito asegura que Symantec Management Agent para UNIX, Linux y Mac pueda detectar fácilmente el servidor web Apache y el archivo de configuración. Si no mueve el directorio de configuración, no deberá especificar ninguna configuración manual adicional.	El directorio de configuración predeterminada es la ubicación que fue compilada en su .exe o **/etc/httpd/conf**.

Si cambia los archivos de configuración del servidor web Apache mientras Symantec Management Agent está en ejecución, los datos se envían a Notification Server después de un período corto. Una vez que los datos del rol del servidor web Apache se envían a Notification Server, el equipo se convierte en el Package Server candidato. Si desea acelerar este proceso deberá ejecutar el archivo ejecutable **aex-sendbasicinventory** manualmente. Ejecute el archivo ejecutable del shell en el equipo cliente al que se apunta para la instalación de Package Server. Actualice Notification Server con los cambios.

Dos ejemplos de configuración están disponibles.

Ver "Ejemplo de configuración de Package Server que usa el directorio web principal para los vínculos de Package Server" en la página 147.

Ver "Ejemplo de la configuración de Package Server usando un alias para los vínculos de Package Server" en la página 150.

Ejemplo de configuración de Package Server que usa el directorio web principal para los vínculos de Package Server

Esta configuración requiere generalmente que se realicen mínimas modificaciones a una instalación predeterminada del servidor web Apache. En esta configuración un directorio virtual que se llama **/Altiris/PS** es creado de forma automática en el directorio HTML principal de Apache.

Ver "Requisitos para configurar HTTPS y HTTP" en la página 146.

La configuración del ejemplo contiene los siguientes directorios:

- **Instantáneas**

- **Paquetes**

Los vínculos simbólicos se establecen en estos directorios para cada paquete compartido. Los paquetes mismos se almacenan en el directorio del Package Server Agent **VAR**.

Esta configuración incluye un servidor HTTP y HTTPS Apache. Package Server usa el servidor HTTPS si está disponible. El servidor HTTPS un garantiza un entorno operativo más seguro y permite el uso de las credenciales de acceso al paquete.

Se realizan varios análisis de archivos de configuración. Los archivos de configuración que se detallan en esta sección son ejemplos. Estos ejemplos son de la instalación predeterminada del servidor web Apache como parte de la distribución de una versión anterior de Red Hat Linux.

Análisis número 1; Instrucción Escuchar es el siguiente:

```
...## When we also provide SSL we have to listen to the ## standard
HTTP port (see above) and to the HTTPS port ## <IfDefine HAVE_SSL>
Listen 80 Listen 443 Listen 10.10.10.10:8080 </IfDefine>...
```

Asegúrese de que la instrucción Escuchar para cada uno de los servidores principales sea la primera instrucción Escuchar de su tipo en el archivo de configuración. Los servidores principales HTTP y HTTPS deben ser las primeras dos instrucciones Escuchar.

Es necesario eliminar el IP o asegurarse de que es el mismo IP al cual el nombre del host se resuelve, según lo informado a Notification Server.

Análisis número 2; Opciones de directorio principales es el siguiente:

```
...

# DocumentRoot: The directory out of which you will serve your
Notification Server Reference 62

# documents. By default, all requests are taken from this directory,
but

# symbolic links and aliases may be used to point to other locations.
DocumentRoot "/var/www/html" ...

# This should be changed to whatever you set DocumentRoot to.

#<Directory "/var/www/html">

# This may also be "None", "All", or any combination of "Indexes",

# "Includes", "FollowSymLinks", "ExecCGI", or "MultiViews".

# Note that "MultiViews" must be named *explicitly* --- "Options All"

# does not give it to you.
```

```
Options Indexes FollowSymLinks

# This controls which options the .htaccess files in directories can

# override. Can also be "All", or any combination of "Options",
"FileInfo",

# "AuthConfig", and "Limit" AllowOverride AuthConfig

# Controls who can get stuff from this server.

Order allow,deny

Allow from all

</Directory>

...
```

Busque el nodo **<Directorio>** para el directorio **DocumentRoot** y asegúrese de que las siguientes opciones estén configuradas:

- **FollowSymLinks**
- **AllowOverride AuthConfig** o **Allow override All**

Análisis número 3; Comprobar host SSL es el siguiente:

```
## SSL Virtual Host Context

<VirtualHost _default_:443>

# General setup for the virtual host

DocumentRoot "/var/www/html"

ErrorLog logs/error_log

TransferLog logs/access_log Notification Server Reference 63

# SSL Engine Switch:

# Enable/Disable SSL for this virtual host.

SSLEngine on

...
```

Asegúrese de que el host virtual SSH de **_default_** tenga el puerto correcto. El puerto debe coincidir con la primera instrucción SSH. Asegúrese de que el directorio DocumentRoot del host virtual sea el mismo que el del servidor principal.

El directorio DocumentRoot del host puede ser diferente del servidor principal. El directorio DocumentRoot del host debe tener un nodo **<Directorio>** configurado con las mismas opciones que se especifican en el análisis número 2.

Ejemplo de la configuración de Package Server usando un alias para los vínculos de Package Server

Es conveniente mantener el directorio virtual de Package Server para Linux totalmente a parte del directorio del servidor web Apache. Para mantenerlos aparte, siga este ejemplo de configuración. Este ejemplo de configuración mantiene todos los vínculos simbólicos fuera del directorio principal del servidor web Apache. Se asegura de que las opciones FollowSymLinks no se necesiten en el directorio principal.

Ver "Requisitos para configurar HTTPS y HTTP" en la página 146.

Un alias se usa en el archivo de configuración del servidor web Apache para separar el directorio virtual **/Altiris/ PS**. Package Server para Linux detecta de forma automática este alias y crea los subdirectorios necesarios en la ubicación correcta.

Los subdirectorios son los siguientes:

- **Paquetes**
- **Instantáneas**

Los paquetes reales se descargan en el directorio **VAR** en el agente.

Los archivos de configuración que se usan en esta sección son un ejemplo. Los ejemplos son de la instalación predeterminada del servidor web Apache como parte de la distribución de una versión anterior de Red Hat Linux.

El **Análisis número 1; Instrucción Escuchar** es el siguiente:

```
...## When we also provide SSL we have to listen to the

## standard HTTP port (see above) and to the HTTPS port

##

<IfDefine HAVE_SSL>

Listen 80

Listen 443

Listen 10.10.10.10:8080

</IfDefine>

...
```

Asegúrese de que la instrucción Escuchar para cada uno de los servidores principales sea la primera instrucción Escuchar de su tipo en el archivo de configuración. Los servidores principales HTTP y HTTPS deben ser las primeras dos instrucciones Escuchar.

Es necesario eliminar el IP o asegurarse de que es el mismo IP al cual el nombre del host se resuelve, según lo informado a Notification Server. Es posible usar los números de puerto con excepción de 80 y de 443. Package Server para Linux detecta los puertos. Sin embargo, usa siempre el puerto de la primera escucha en el archivo de configuración del servidor web Apache.

Análisis número 2; Crear alias y opciones de directorio de alias es el siguiente:

```
...
# Aliases: Add here as many aliases as you need (no limit). The format
is
# Alias fakename realname
#
<IfModule mod_alias.c>
...
Alias /Altiris/PS /var/altiris/www/ps
<Directory /var/altiris/www/ps >
Options FollowSymLinks
AllowOverride All
</Directory> </IfModule>
# End of aliases.
```

Es necesario realizar estos pasos en el orden siguiente:

- Cree la instrucción Alias y el nodo **<Directorio>** para el directorio de destino del alias.
- Asegúrese de que las siguientes opciones estén configuradas en ese directorio:
  - **FollowSymLinks**
  - **AllowOverride AuthConfig** o **Allow override All**
- Cree el directorio de destino.
- Configure los permisos correctos en el directorio de destino para asegurarse de que los clientes de servidor web Apache puedan descargar los archivos de allí.
- Para asegurarse de que el directorio funcione, coloque un archivo de texto en él. A continuación vaya a una URL tal como http://your.server.name/Altiris/PS/testfile.txt. En este ejemplo, your.server.name y testfile.txt son su propio nombre de servidor y el nombre del archivo de texto que usted creó.

Análisis número 3; Comprobar host SSL es el siguiente:

```
...

## SSL Virtual Host Context

<VirtualHost _default_:443>

# General setup for the virtual host

DocumentRoot "/var/www/html"

ErrorLog logs/error_log

TransferLog logs/access_log

# SSL Engine Switch:

# Enable/Disable SSL for this virtual host.

SSLEngine on

...
```

Asegúrese de que el host virtual SSH de **_default_** tenga el puerto correcto. Debe coincidir con la primera instrucción SSH. Asegúrese de que su directorio DocumentRoot sea el mismo que el del servidor principal.

Capítulo 8

Configuración de la jerarquía

En este capítulo se incluyen los temas siguientes:

- Acerca de la jerarquía de Notification Server
- Requisitos de la jerarquía
- Implementar la jerarquía de Notification Server

Acerca de la jerarquía de Notification Server

La jerarquía es una tecnología diseñada para reducir el costo total de propiedad (TCO, Total Cost of Ownership) de administrar el software y las soluciones de Symantec a través de varios equipos Notification Server. La jerarquía reduce el costo total de propiedad al complementar el sistema de Notification Server con capacidades de administración centralizada.

Ver "Requisitos de la jerarquía" en la página 155.

Ver "Implementar la jerarquía de Notification Server" en la página 156.

La jerarquía define el flujo de información entre varios equipos Notification Server de una empresa. Si tiene varios equipos Notification Server, puede usar la jerarquía para definir las colecciones de equipos Notification Server que comparten una configuración y datos comunes. La jerarquía puede distribuir y sincronizar cualquier cambio que se realice a la configuración y a los datos compartidos. La jerarquía permite administrar las soluciones de Symantec a través de varios equipos Notification Server desde una ubicación central.

Algunas soluciones, como Inventory Solution, Patch Management Solution y Software Management Solution, están configuradas para participar en la jerarquía.

Para obtener información sobre una solución específica, consulte la documentación de la solución correspondiente.

La jerarquía usa la replicación para copiar y para sincronizar objetos y datos compartidos entre los equipos Notification Server dentro de la misma estructura jerárquica. En intervalos programados, cada servidor de una jerarquía sincroniza objetos y datos con su servidor principal y servidor secundario inmediato.

Ver "Acerca de la replicación y las reglas de replicación" en la página 172.

Una topología de jerarquía define las relaciones entre Notification Servers, que a su vez controla cómo ocurre la sincronización entre nodos adyacentes.

Una topología de jerarquía cumple con las reglas siguientes:

- Cada Notification Server puede tener cero o un servidor principal.
- Cada Notification Server puede tener cero o más servidores secundarios.

En la jerarquía, los objetos y los datos deben replicarse en direcciones conocidas, de forma que la sincronización es confiable y escalable. Como la jerarquía replica solamente cada objeto o cada dato en una dirección, la administración del conflicto es mínima, y el origen siempre tiene prioridad.

Tabla 8-1 Objetos que se pueden sincronizar entre equipos Notification Server

Objeto	Descripción
Elementos de configuración y administración	Las políticas, las tareas, los filtros y los informes se replican hacia abajo en una jerarquía. Ver "Acerca de cómo ejecutar tareas en jerarquía" en la página 413.
Configuración de seguridad	Los roles de seguridad, los privilegios y los permisos se replican hacia abajo en una jerarquía.
Recursos	La información del recurso, como los equipos, los usuarios, los sitios y sus clases de datos asociados, se replica hacia arriba o hacia abajo en una jerarquía.
Paquetes	Los paquetes que se asocian a los recursos de software, y las clases de datos que se asocian a los paquetes se replican hacia abajo en una jerarquía.
Sucesos	Las clases de suceso, como la ejecución de Software Delivery, se replican hacia arriba o hacia abajo en una jerarquía.

Nota: Algunas soluciones de Symantec crean reglas de replicación personalizadas para garantizar que los elementos específicos siempre estén sincronizados.

Requisitos de la jerarquía

Para compartir o recibir opciones y datos comunes de configuración en varios equipos con Notification Server, primero debe agregar el equipo con Notification Server a una jerarquía. Debido a que los equipos con Notification Server pueden administrarse localmente, cada equipo con Notification Server debe agregarse o eliminarse en la jerarquía de forma individual con las credenciales de acceso correspondientes. Generalmente, el administrador de Symantec que administra el diseño de la topología obtiene acceso de forma remota a los equipos con Notification Servers de otros sitios para agregarlos a la jerarquía.

Ver "Acerca de la jerarquía de Notification Server" en la página 153.

Ver "Implementar la jerarquía de Notification Server" en la página 156.

Los requisitos para configurar la jerarquía son los siguientes:

- El tráfico de red debe ser enrutable entre los equipos con Notification Server contiguos dentro de la jerarquía.
- El tráfico de HTTP/HTTPS debe permitirse entre los equipos con Notification Server contiguos dentro de la jerarquía.
- Si usa los certificados autofirmados para los equipos con Notification Server, asegúrese de que la confianza entre esos equipos esté establecida. Para hacerlo, en **Microsoft Management Console**, en el almacén **Certificados (equipo local)**, instale manualmente los certificados en **Entidad de certificación de raíz de confianza**.
- Deben existir relaciones de confianza entre los equipos con Notification Server contiguos dentro de la jerarquía o deben conocerse las credenciales de las cuentas privilegiadas que faciliten la confianza.
- Cada equipo con Notification Server debe poder determinar el nombre y la dirección de red de cualquier equipo con Notification Server contiguo dentro de la jerarquía.
- Debe haber suficiente ancho de banda entre los sitios con Notification Server para admitir la replicación de datos y de paquetes.
  El ancho de banda y el hardware que se requieren dependen del tamaño de la topología de jerarquía y de los datos replicados.
- Debe existir un sitio para cada equipo con Notification Server, el cual debe incluir la subred que contiene Notification Server. El sitio también debe contener

un servidor de paquetes (un servidor de sitio que ejecute el servicio de administración de paquetes) que dé servicio al equipo con Notification Server. Ver "Acerca de los servicios de sitio" en la página 127.

Implementar la jerarquía de Notification Server

Para compartir o recibir datos y opciones de configuración comunes con varios Notification Servers, es necesario agregar el equipo con Notification Server a una jerarquía y configurar las reglas de replicación necesarias.

Tabla 8-2 Proceso para implementar la jerarquía de Notification Server

Paso	Acción	Descripción
Paso 1	Crear las relaciones jerárquicas correspondientes entre los Notification Servers.	Crea una jerarquía al generar una serie de relaciones de principal a secundario y de secundario a principal que vinculan los equipos con Notification Server en su sistema. Ver "Creación y administración de relaciones jerárquicas" en la página 157. Ver "Configurar una relación jerárquica entre dos equipos con Notification Server" en la página 161.
Paso 2	Crear y habilitar las reglas de replicación adecuadas para especificar los datos que desee replicar a lo largo de la jerarquía.	La réplica de la jerarquía de recursos y eventos se configura mediante reglas de replicación. Estas reglas definen los datos que desea replicar en otros Notification Servers. Ver "Configurar la réplica de la jerarquía y las reglas de la réplica de la jerarquía" en la página 163. Si desea configurar una réplica de la jerarquía personalizada para elementos de configuración y administración, especifique la configuración apropiada. Ver "Cómo configurar una réplica de la jerarquía personalizada" en la página 165.

Paso	Acción	Descripción
Paso 3	(Opcional) Realice tareas de replicación manuales.	Normalmente, los equipos con Notification Server de una jerarquía se sincronizan conforme a la programación de replicación que se haya configurado en las reglas de replicación. No obstante, puede anular de forma manual la programación de replicación diferencial de Notification Server y activar las reglas de réplica de la jerarquía de inmediato. Ver "Cómo anular la programación de réplica diferencial de jerarquía" en la página 167. Puede replicar datos seleccionados de forma manual directamente desde Notification Server a todos sus Notification Servers secundarios sin incluir esto en una regla de replicación. La réplica manual es una réplica única que se realiza de inmediato. Necesita tener permiso de lectura en la acción del elemento del menú contextual **Replicar ahora** para realizar la replicación manual. Ver "Cómo replicar datos seleccionados manualmente" en la página 168.
Paso 4	(Opcional) Configure políticas de automatización de jerarquía.	Las políticas de automatización de jerarquía envían notificaciones por correo electrónico cuando ocurren ciertos eventos en la jerarquía. Ver "Configurar una política de automatización de jerarquía" en la página 168.
Paso 5	Ejecute un informe de jerarquía.	Puede ejecutar un informe en cualquier Notification Server de la jerarquía a fin de extraer datos de su CMDB. Actualice los datos de resumen antes de ejecutar un informe de jerarquía. Ver "Cómo ejecutar un informe de jerarquía" en la página 169. Ver "Cómo actualizar datos de resumen" en la página 170.

Ver "Acerca de la jerarquía de Notification Server" en la página 153.

Ver "Requisitos de la jerarquía" en la página 155.

Creación y administración de relaciones jerárquicas

Crea una jerarquía al generar una serie de relaciones de principal a secundario y de secundario a principal que vinculan los equipos con Notification Server en su sistema. Puede agregar su Notification Server (en el cual ha iniciado sesión, que puede ser remota) a una jerarquía como secundario de un Notification Server remoto existente o como su principal.

Puede agregar su Notification Server (en el cual ha iniciado sesión, que puede ser remota) a una jerarquía como secundario de un Notification Server remoto existente o como su principal. Para crear una relación jerárquica, necesita una cuenta de administrador de Symantec (o una cuenta con privilegios equivalentes) en ambos equipos. Para agregar o quitar equipos con Notification Server de una jerarquía, necesita el privilegio **Administrar la topología de jerarquía** en el equipo con Notification Server donde se realiza la acción.

Puede ver y configurar la jerarquía del equipo con Notification Server mediante Symantec Management Console. Si usted es el administrador de la jerarquía, solamente puede ver el servidor principal y los secundarios (y todos los niveles inferiores) del Notification Server.

Tenga en cuenta que todas las acciones que realice se basan en su Notification Server. Si hace clic con el botón derecho en un equipo con Notification Server no se le permitirá que inicie sesión de forma remota en ningún equipo remoto con Notification Server. Se abre un menú contextual que contiene las acciones que puede realizar en ese servidor, las cuales son diferentes para los equipos locales y remotos. Existe un amplio conjunto de acciones disponibles para el servidor local, mientras que para los servidores remotos las acciones son limitadas. Las acciones tales como la extracción de informes se realizan en la base de datos correspondiente.

Las acciones que puede realizar en la jerarquía son relativas a su equipo con Notification Server, que es el equipo al cual está conectado. Si posee el privilegio **Administrar historial** en un equipo remoto con Notification Server, puede iniciar sesión de forma remota en ese equipo. Podrá entonces abrir Symantec Management Console y realizar la configuración de jerarquía relativa a ese equipo.

Puede habilitar o deshabilitar la réplica de la jerarquía en determinados equipos con Notification Server en cualquier momento. Por ejemplo, puede usar esta función para deshabilitar de forma temporal la réplica de la jerarquía durante las tareas de mantenimiento, tales como la instalación, la actualización o la desinstalación de la solución. La deshabilitación de la replicación en un equipo con Notification Server no afecta la programación de réplicas en los demás equipos con Notification Server de la jerarquía. No obstante, no se pasan datos a través del equipo deshabilitado de modo que la replicación descendente se detiene en el servidor principal, y la replicación ascendente se detiene en los secundarios.

El símbolo de color en la página **Administración de jerarquía** indica todas las alertas de jerarquía. Los colores que posiblemente vea y su correspondiente estado de alerta son los siguientes:

Amarillo	Estado de alerta bajo.
Naranja	Estado de alerta medio.

Rojo	Estado de alerta crítico Por ejemplo, si intenta replicar los mismos datos tanto hacia arriba como hacia abajo de la jerarquía desde el mismo Notification Server, se levanta una alerta crítica. Los datos deben replicarse solamente en una dirección. Si el equipo principal o secundario con Notification Server tiene las mismas reglas de réplica de la jerarquía implementadas, puede configurar un conflicto de datos.

Esta tarea es un paso en el proceso para implementar la jerarquía de Notification Server.

Ver "Implementar la jerarquía de Notification Server" en la página 156.

Para crear y administrar relaciones jerárquicas

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Notification Server > Jerarquía**.
2. En la página **Administración de jerarquía**, en la ficha **Topología**, en la lista desplegable **Ver**, haga clic en **Diagrama** para visualizar la jerarquía en formato gráfico.

   Use la vista **Cuadrícula** solamente para copiar los datos al portapapeles. Contiene datos que no se muestran en la vista **Diagrama**.

3 Realice cualquiera de las siguientes tareas:

Agregar un nuevo Notification Server a la jerarquía	Ver "Configurar una relación jerárquica entre dos equipos con Notification Server" en la página 161.
Modificar una relación jerárquica entre dos Notification Servers	Ver "Configurar una relación jerárquica entre dos equipos con Notification Server" en la página 161.
Eliminar un Notification Server de la jerarquía	Haga clic con el botón derecho en el equipo con Notification Server que desee quitar y después haga clic en **Quitar**.
Habilitar o deshabilitar la réplica de la jerarquía	Es probable que desee deshabilitar la participación en la jerarquía cuando realice el mantenimiento en un Notification Server. Haga clic con el botón derecho en el equipo con Notification Server en el que desee habilitar o deshabilitar la réplica de la jerarquía y haga clic en **Habilitar replicación** o **Deshabilitar replicación**, según corresponda. La deshabilitación de la réplica de la jerarquía afecta solamente la programación de la réplica de jerarquía. No tiene efecto sobre ninguna réplica independiente que se haya configurado en Notification Server o desde otro servidor. La sincronización manual de la jerarquía no cambia esta configuración, sino que la sobrescribe para realizar una única réplica de los elementos correspondientes.
Sobrescribir manualmente la programación de la réplica de la jerarquía de un Notification Server	Ver "Cómo anular la programación de réplica diferencial de jerarquía" en la página 167.
Ejecutar un informe de jerarquía	Ver "Cómo ejecutar un informe de jerarquía" en la página 169.

4 Haga clic en **Guardar cambios**.

Ver "Acerca de la jerarquía de Notification Server" en la página 153.

Ver "Requisitos de la jerarquía" en la página 155.

Video: Para obtener más información acerca de cómo configurar una jerarquía, consulte Video de configuración de una jerarquía en IT Management Suite en Symantec Connect.

Configurar una relación jerárquica entre dos equipos con Notification Server

Es posible configurar una relación jerárquica (servidor principal o servidor secundario) entre su equipo con Notification Server y un equipo remoto con Notification Server. Es necesario especificar el nombre, la URL (que debe incluir cualquier configuración de puertos o HTTPS no predeterminadas) y los detalles del acceso del equipo remoto con Notification Server. Usted además necesita proporcionar los detalles del acceso de su equipo local con Notification Server. De forma predeterminada, la programación de réplica de la jerarquía escalona la replicación entre cada par de equipos con Notification Server Es posible cambiar la programación de la replicación para adaptarse a sus requisitos, pero se debe asegurar que se mantenga el escalonamiento de replicación.

Ambos equipos con Notification Server deben tener un Package Server disponible en los sitios respectivos. Se requiere un servidor de paquetes por motivos de rendimiento. No es posible crear una relación jerárquica entre dos equipos con Notification Server si alguno no tiene un Package Server disponible.

Las credenciales de la aplicación de Notification Server deben ser estables y no se las debe cambiar regularmente como algunas contraseñas de cuenta de usuario. Si la contraseña de cuenta de la aplicación del equipo con Notification Server deja de ser válida, aparece un mensaje en la consola. El mensaje solicita usar la herramienta de línea de comandos ASConfig para hacer las actualizaciones necesarias.

Esta tarea es un paso en el proceso para implementar la jerarquía de Notification Server.

Ver "Implementar la jerarquía de Notification Server" en la página 156.

Para configurar una relación jerárquica entre dos equipos con Notification Server

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Administración de Notification Server > Jerarquía**.
2. En la página Administración de jerarquía, en la ficha **Topología**, haga clic con el botón derecho en su Notification Server y después haga clic en la opción apropiada:
   - **Agregar > Principal**
   - **Agregar > Secundario**

3 En el **Asistente para agregar nodos de jerarquía**, en la página **Notification Server**, escriba el nombre, la URL y las credenciales de acceso del equipo con Notification Server remoto.

Las credenciales de acceso deben ser una cuenta de administrador de Symantec o una cuenta equivalente en el equipo remoto con Notification Server.

4 Haga clic en **Opciones avanzadas**.

5 En el cuadro de diálogo **Devolver la configuración de credenciales**, especifique la cuenta de administrador de Symantec (o equivalente) que usa el equipo remoto con Notification Server para comunicarse con el equipo local con Notification Server y, luego, haga clic en **Aceptar**.

6 En el **Asistente para agregar nodos de jerarquía**, haga clic en **Siguiente**.

7 En la página **Programaciones de replicación**, configure las programaciones de replicación diferencial y completa, habilite las que desee usar en el equipo con Notification Server y, luego, haga clic en **Siguiente**.

De forma predeterminada, solamente la programación de réplica diferencial está habilitada. La replicación completa se usa raramente porque pone una carga pesada en el equipo con Notification Server, pero se la puede habilitar cuando sea necesario. Es necesario programar la replicación para las horas que no coincidan con programaciones de réplica en otros equipos con Notification Server de la jerarquía.

Ver "Cómo administrar programaciones compartidas" en la página 122.

Ver "Configuración de una programación" en la página 123.

8 En la página **Confirmar opciones**, verifique que la configuración sea correcta y después haga clic en **Terminar**.

El equipo local con Notification Server usa la información especificada para localizar y verificar el equipo remoto con Notification Server y configurar la relación jerárquica apropiada con este.

Si el equipo remoto con Notification Server no tiene un Package Server disponible en el sitio, la verificación falla y la relación jerárquica no se puede establecer.

Ver "Acerca de la jerarquía de Notification Server" en la página 153.

Ver "Requisitos de la jerarquía" en la página 155.

Configurar la réplica de la jerarquía y las reglas de la réplica de la jerarquía

La réplica de la jerarquía especifica lo que se replica en la jerarquía. No tiene efecto en la replicación independiente que puede configurar entre dos Notification Servers.

Si agrega un Notification Server a la jerarquía, puede especificar lo que se replica en el Notification Server principal y en los Notification Servers secundarios. De forma predeterminada, se replica todo (replicación completa), lo que puede consumir demasiado ancho de banda. Symantec recomienda que configure la réplica de la jerarquía en cada Notification Server para que se adapte mejor a los requisitos de su organización.

Nota: La replicación no se admite entre dos Notification Servers que tienen diferentes versiones de IT Management Suite instaladas. Por ejemplo, no se puede replicar datos de un servidor 7.0 a un servidor 7.1.

Cualquier dato que se replique hacia abajo de un Notification Server principal tiene prioridad y sobrescribe los datos correspondientes en los servidores secundarios. Los elementos de configuración y administración replicados que se reciben de un servidor principal por lo general son de solo lectura y no se pueden modificar. La configuración de solo lectura permite que se repliquen sin modificar hacia abajo en la jerarquía. Si desea permitir incorporaciones a los elementos replicados en los servidores secundarios, debe desbloquear los elementos relevantes en el equipo con Notification Server en el cual fueron creados. Por ejemplo, quizá desee aplicar las políticas para que se habiliten y deshabiliten en los Notification Servers secundarios.

La réplica de la jerarquía de recursos y eventos se configura mediante reglas de replicación. Estas reglas definen los datos que desea replicar a otros Notification Servers. Cada regla replica los datos especificados en una dirección solamente, hacia arriba al Notification Server principal o hacia abajo a los Notification Server secundarios. Si configura dos reglas en las cuales se replique el mismo tipo de recurso en ambas direcciones, se emite una alerta crítica y no se ejecutan las reglas de replicación.

Es posible incluir los destinos del recurso en una regla de replicación del recurso. El ámbito del recurso se aplica al contenido (los recursos) de los destinos que se replican. Por lo tanto, los recursos que se replican dependen del propietario del destino de recursos. El administrador de Notification Server puede elegir replicar los recursos de destino en su estado actual (poseídos por alguien más, con el ámbito correspondiente). De forma alternativa, puede tomar posesión de los destinos, guardarlos con el ámbito del administrador (el cual, por lo general, contiene más recursos) y replicarlos en ese estado. Se replican todos los miembros actuales

del destino de recurso. El elemento de destino de recurso real se replica en segundo plano como elemento dependiente. Por ejemplo, cuando una regla de replicación se crea en el servidor principal que se aplica a un recurso de destino. El recurso de destino se replica como un elemento dependiente cuando la regla de replicación misma se replica hacia abajo en la jerarquía.

La jerarquía tiene dos modos de réplica:

Diferencial	Replica los objetos y los datos que se han modificado desde la última replicación. Este modo se habilita de forma predeterminada y reduce la carga y el ancho de banda que la jerarquía utiliza.
Completa	Replica todos los objetos y datos. Este modo se encuentra deshabilitado de forma predeterminada.

Para minimizar la carga en la red y evitar colisiones entre los datos, debe programar la réplica de la jerarquía a una hora distinta para cada Notification Server de la jerarquía.

Ver "Configuración de una programación" en la página 123.

La réplica de la jerarquía sincroniza los distintos tipos de objetos de los modos siguientes:

Objetos de seguridad	Los objetos de seguridad, tales como las funciones y los privilegios, siempre utilizan réplicas completas. La réplica diferencial no es una opción para los objetos de solo lectura como estos.
Elementos	Los elementos utilizan la réplica diferencial, la cual es manejada realizando un hash en cada elemento para verificar los cambios y replicando los que hayan cambiado.
Recursos	Los recursos utilizan la réplica diferencial. La réplica diferencial se basa en la fecha y hora "de última modificación" en los datos de origen. Cualquier dato que haya cambiado desde la última réplica se replica en el servidor de destino. A continuación, se verifican los datos del destino, si se ha habilitado la verificación de datos en la regla de replicación adecuada. La verificación de datos impone una carga de procesamiento considerable en Notification Server. Para reducir dicha carga, verifique el porcentaje de datos especificado en el servidor de destino con cada réplica. Por ejemplo, si se verifica el 10% de los datos para cada replicación, se garantiza que todos los datos se hayan verificado después de 10 replicaciones.

Esta tarea es un paso en el proceso para implementar la jerarquía de Notification Server.

Ver "Implementar la jerarquía de Notification Server" en la página 156.

Para configurar la réplica de la jerarquía y las reglas de la réplica de la jerarquía

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Notification Server > Jerarquía**.
2. En la página **Administración de jerarquía**, seleccione la ficha **Replicación**.
3. Configure la réplica de la jerarquía seleccionando las opciones adecuadas.

   Para obtener más información, haga clic en la página y después presione **F1**.
4. Para configurar las reglas de la réplica de la jerarquía, realice una de las siguientes acciones:

Cree una nueva regla de la réplica de la jerarquía	1 Haga clic en **Agregar**. 2 En el cuadro de diálogo **Regla de replicación**, especifique la configuración apropiada. Para obtener más información, haga clic en la página y después presione **F1**. 3 Haga clic en **Guardar cambios**.
Modifique una regla de la réplica de la jerarquía existente	1 Seleccione la regla apropiada y, a continuación, haga clic en **Editar**. 2 En el cuadro de diálogo **Regla de replicación**, especifique la configuración apropiada. 3 Haga clic en **Guardar cambios**.
Habilite una regla de la réplica de la jerarquía	Seleccione **Habilitada** junto al nombre de la regla de replicación.
Elimine una regla de la réplica de la jerarquía	Seleccione la regla apropiada y, a continuación, haga clic en **Eliminar**. Las reglas de replicación que se proporcionan con Notification Server o las soluciones instaladas no pueden ser eliminadas. No obstante, puede habilitar y deshabilitar estas reglas cuando sea necesario, y puede editar el nombre y la descripción de la regla.

5. Haga clic en **Guardar cambios**.

Cómo configurar una réplica de la jerarquía personalizada

Es posible configurar una réplica de la jerarquía personalizada para los elementos de configuración y de administración, y los roles de seguridad y los privilegios.

El informe de replicación del elemento actual al que se puede acceder desde el panel Elementos de configuración y administración muestra todos los elementos que se han habilitado para la replicación usando la réplica de la jerarquía personalizada. Cuando se replican los elementos seleccionados, se incluye automáticamente cualquier elemento dependiente que no se haya habilitado. Estos elementos no aparecen en el informe de replicación del elemento. Para ver una lista de todos los elementos que fueron replicados, es necesario ver el informe de objetos replicados.

Esta tarea es un paso en el proceso para implementar la jerarquía de Notification Server.

Ver "Implementar la jerarquía de Notification Server" en la página 156.

Para configurar una réplica de la jerarquía personalizada para los elementos de configuración y administración

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Notification Server > Jerarquía**.
2. En la página **Administración de jerarquía**, en la ficha **Replicación**, en el panel **Elementos de configuración y administración**, haga clic en **Personalizado(a)**.
3. Haga clic en **Guardar cambios**.
4. En Symantec Management Console, en el panel izquierdo, haga clic con el botón derecho en la carpeta o el elemento que desee replicar y después haga clic en **Jerarquía > Habilitar replicación**.
5. Si ha seleccionado una carpeta, en el cuadro de diálogo **Funcionamiento de replicación heredado**, especifique si desea incluir el contenido de la carpeta en la replicación:

Para incluir todo el contenido de la carpeta	Haga clic en **Sí**.
Para replicar solamente la carpeta sin contenido	Haga clic en **No**.

Si es necesario, se pueden habilitar o deshabilitar manualmente subcarpetas determinadas más tarde.

Para instalar la réplica de la jerarquía personalizada para los roles de seguridad y los privilegios

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Notification Server > Jerarquía**.
2. En la página **Administración de jerarquía**, en la ficha **Replicación**, en **Seguridad**, haga clic en **Personalizado(a)**.
3. Haga clic en **Seleccionar roles y privilegios de seguridad**.
4. En la ventana **Seleccionar roles y privilegios de seguridad**, seleccione los roles y los privilegios que desee replicar.
5. Haga clic en **Aceptar**.
6. Haga clic en **Guardar cambios**.

Cómo anular la programación de réplica diferencial de jerarquía

Normalmente, los equipos con Notification Server de una jerarquía se sincronizan conforme a la programación de replicación que se haya configurado en las reglas de replicación. De ser necesario, puede sobrescribir de forma manual la programación de réplicas diferenciales de Notification Server y activar las reglas de réplica de la jerarquía de inmediato. Activa la programación diferencial de jerarquía en el nodo secundario seleccionado. Cualquier regla de réplica de la jerarquía que se configura para ejecutarse en la programación diferencial se ejecuta de forma inmediata. Cualquier regla configurada para ejecutarse en programaciones personalizadas no se activa para ejecutarse simultáneamente. Puede replicar los datos de forma manual en el Notification Server solamente a partir de un servidor principal remoto o de un Notification Server secundario.

No se puede sobrescribir de forma manual la réplica en un Notification Server remoto. Solamente se puede realizar una operación que afecte al equipo con Notification Server Puede iniciar sesión en un equipo con Notification Server remoto para que sea su Notification Server y anular manualmente las programaciones de réplica diferencial en el Notification Server principal o en los secundarios.

Esta tarea es un paso en el proceso para implementar la jerarquía de Notification Server.

Ver "Implementar la jerarquía de Notification Server" en la página 156.

Para anular la programación de réplica diferencial de jerarquía

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Notification Server > Jerarquía**.
2. En la página **Administración de jerarquía**, en la ficha **Topología**, haga clic con el botón derecho en el equipo con Notification Server desde el cual desea replicar datos.
3. Haga clic en **Jerarquía > Réplica para…**.

   Esta opción activa las reglas de réplica de la jerarquía que señalan el Notification Server local (en el cual ha iniciado sesión). No puede replicar los datos del Notification Server remoto en ningún otro servidor remoto.
4. En el cuadro de diálogo de confirmación, haga clic en **Aceptar**.

Cómo replicar datos seleccionados manualmente

Para sobrescribir las reglas de replicación del Notification Server, realice una réplica de la jerarquía manual de una carpeta o de un elemento en particular. La replicación manual replica los datos seleccionados en los servidores secundarios Notification Server de inmediato. Los datos se reproducen independientemente de las programaciones de réplica o de si los datos se hayan incluido en las reglas de replicación.

Esta tarea es un paso en el proceso para implementar la jerarquía de Notification Server.

Ver "Implementar la jerarquía de Notification Server" en la página 156.

Para replicar los datos seleccionados de forma manual a partir de Notification Server

1. En Symantec Management Console, en el panel izquierdo, haga clic con el botón derecho en la carpeta o en el elemento que desee replicar.

   Si selecciona una carpeta, la replicación incluye todo su contenido (todos los niveles de subcarpetas y elementos que contiene). También se replican todas las carpetas principales (pero no su contenido) a fin de conservar las rutas de carpeta dentro de la estructura.
2. Haga clic en **Jerarquía > Replicar ahora…**.
3. En el cuadro de diálogo de confirmación, haga clic en **Aceptar**.

Configurar una política de automatización de jerarquía

Las políticas de automatización de jerarquía envían notificaciones por correo electrónico cuando ocurren ciertos eventos en la jerarquía. Es necesario activar

las políticas que desee usar. Tenga en cuenta que no puede modificar las políticas predeterminadas, pero es posible clonarlas para crear nuevas políticas. A continuación, puede configurar las políticas que se adapten a sus necesidades.

Esta tarea es un paso en el proceso para implementar la jerarquía de Notification Server.

Ver "Implementar la jerarquía de Notification Server" en la página 156.

Para configurar una política de automatización de la jerarquía

1. En Symantec Management Console, en el menú **Administrar**, haga clic en **Políticas de automatización**.
2. En el panel izquierdo, haga clic en una de las siguientes políticas:

Alertas críticas de jerarquía	Envía una alerta de prioridad alta por correo electrónico al administrador de Notification Server siempre que se recibe una alerta crítica en el Notification Server local. Los estados de las alertas críticas también se indican en la ficha **Topología** en la página Administración de jerarquía.
Habilitar o deshabilitar la jerarquía	Envía una alerta de prioridad alta por correo electrónico al administrador de Notification Server siempre que se habilita o deshabilita la réplica de jerarquía en el Notification Server local.
Alertas altas de jerarquía	Envía una alerta de prioridad alta por correo electrónico al administrador de Notification Server siempre que se recibe una alerta de prioridad alta en el Notification Server local.
Cambio de la estructura de jerarquía	Envía una alerta de prioridad alta por correo electrónico al administrador de Notification Server siempre que se agrega o se elimina un Notification Server de la jerarquía.

3. En el panel derecho, especifique la configuración de la política y, después, haga clic en **Guardar cambios**.
4. En la barra de herramientas, haga clic en **Activar**.

Cómo ejecutar un informe de jerarquía

Puede ejecutar un informe en cualquier Notification Server de la jerarquía a fin de extraer datos de su CMDB. Es posible que desee actualizar los datos de resumen antes de ejecutar un informe de jerarquía. Es posible actualizar los datos de resumen cuando lo necesite o programar las actualizaciones.

Ver "Cómo actualizar datos de resumen" en la página 170.

Algunas soluciones instaladas podrían proporcionar informes federados de jerarquía. Estos informes resumen los datos relevantes a través de la jerarquía y los resultados contienen una sola línea para cada Notification Server. Puede ejecutar el informe completo en un Notification Server particular o hacer doble clic en la línea correspondiente.

Esta tarea es un paso en el proceso para implementar la jerarquía de Notification Server.

Ver "Implementar la jerarquía de Notification Server" en la página 156.

Para ejecutar un informe de jerarquía

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Notification Server > Jerarquía**.
2. En la página **Administración de jerarquía**, en la ficha **Topología**, haga clic con el botón derecho en el equipo con Notification Server en el cual desee ejecutar un informe.
3. Haga clic en **Informes** y, luego, en el informe apropiado.
4. En la página del informe, especifique cualquier parámetro que desee utilizar y actualice el informe.

   Ver "Cómo extraer resultados del informe de Notification Server" en la página 441.

Cómo actualizar datos de resumen

Si es necesario generar los datos para los informes habilitados para la jerarquía, se puede actualizar datos de resumen en Task Server. Es posible actualizar los datos de resumen a petición, programar una actualización de una vez o crear una programación personalizada para las actualizaciones que se repiten.

Una programación predeterminada ejecuta la tarea de forma automática diariamente. Si desea las actualizaciones diarias de los datos de inventario, no deberá cambiar la programación de la actualización.

Esta tarea es un paso en el proceso para implementar la jerarquía de Notification Server.

Ver "Implementar la jerarquía de Notification Server" en la página 156.

Para actualizar los datos de resumen a petición

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Todas las configuraciones**.
2. En el panel izquierdo, expanda **Notification Server > Configuración de tareas > Actualizar datos de resumen**.

3 En la página **Actualizar datos de resumen**, haga clic con el botón derecho en la tarea que desee ejecutar y haga clic en **Iniciar ahora**.

Es posible hacer clic en **Detalles** para obtener más información sobre la tarea antes de que la ejecute.

4 Si la programación que desee ejecutar no está en la lista, cree una programación personalizada.

Para crear una programación

1 En Symantec Management Console, en el menú **Configuración**, haga clic en **Todas las configuraciones**.

2 En el panel izquierdo, expanda **Notification Server > Configuración de tareas > Actualizar datos de resumen**.

3 En la página de **Actualizar datos de resumen**, haga clic en **Nueva programación**.

4 En el cuadro de diálogo **Nueva programación**, especifique la configuración de la programación y después haga clic en **Programación**.

Para obtener más información, haga clic en la página y después presione **F1**.

Ver "Cómo ejecutar un informe de jerarquía" en la página 169.

Capítulo 9

Configuración de la replicación

En este capítulo se incluyen los temas siguientes:

- Acerca de la replicación y las reglas de replicación
- Requisitos de replicación
- Configuración de las reglas de replicación

Acerca de la replicación y las reglas de replicación

La replicación es la transferencia unidireccional de datos entre dos Notification Servers.

Ver "Requisitos de replicación" en la página 174.

Nota: La replicación no se admite entre dos Notification Servers que tienen diferentes versiones de IT Management Suite instaladas. Por ejemplo, no se puede replicar datos de un servidor 7.0 a un servidor 7.1.

Las funciones de replicación independientes que se describen en el presente documento son diferentes de la réplica de la jerarquía. La replicación independiente define el flujo de información entre dos Notification Servers. La réplica de la jerarquía proporciona sincronización de datos confiable y escalable entre varios equipos con Notification Server.

La replicación se puede configurar para replicar datos fuera de la estructura de jerarquía. Por ejemplo, enviando datos a un servidor externo que clasifica información determinada para informes.

Se admiten los siguientes tipos de replicación:

Diferencial	Replica los objetos y los datos que se han modificado desde la última replicación. Este es el método recomendado porque reduce la carga de red y el consumo de ancho de banda cuando se replican datos.
Completa	Replica todos los objetos y datos. Este método se usa generalmente para la réplica de la jerarquía. Una replicación completa se realiza típicamente mensualmente para asegurar la replicación completa. La replicación independiente no realiza la replicación completa como hace la réplica de jerarquía. La replicación independiente es siempre diferencial.

Otra diferencia entre la réplica de la jerarquía y la replicación es que, en una jerarquía, se aseguran los datos replicados y (de forma predeterminada) son de solo lectura. La propiedad se aplica de modo que los equipos con Notification Server secundarios no puedan sobrescribir automáticamente los datos que se han replicado desde los equipos con Notification Server principales. Algunos datos incluyen la configuración que permite que se los pueda editar en el destino y se los puede configurar según sea necesario. La replicación no tiene propiedad, de forma que todos los datos replicados se pueden editar en los equipos con Notification Server de destino.

Para configurar la replicación, debe configurar las reglas de replicación apropiadas en cada equipo con Notification Server. Cada regla especifica los datos que se replicarán del servidor (el servidor de origen) a uno o más servidores de destino especificados y la programación que se utilizará.

Ver "Configuración de las reglas de replicación" en la página 175.

Es posible crear una regla de replicación para los siguientes elementos:

Eventos	Replica eventos de Notification Server.
Elementos	Replica elementos de configuración y administración de Notification Server, como políticas, filtros e informes.

Recursos	Replica tipos de recursos, destinos de recursos y clases de datos específicas de Notification Server. Si incluye los destinos de recursos en una regla de replicación del recurso, recuerde que la determinación del ámbito del recurso se aplica a los contenidos (recursos) del destino replicado. Por lo tanto, los recursos que se replican dependen del propietario del destino de recursos. El administrador de Notification Server puede elegir replicar los recursos de destino en su estado actual (poseídos por alguien más, con el ámbito correspondiente). De forma alternativa, puede tomar posesión de los destinos, guardarlos con el ámbito del administrador (el cual, por lo general, contiene más recursos) y replicarlos en ese estado. Se replican todos los miembros actuales del destino de recurso. El elemento de destino de recurso real se replica en segundo plano como elemento dependiente. El destino aplicado a una regla independiente se replica cuando la regla independiente se replica a sí misma. Cuando la regla se ejecuta, el destino no se envía.
Seguridad	Replica funciones y privilegios de seguridad de Notification Server. Hay disponibles dos tipos de reglas de replicación de seguridad. De Privilegio y de rol. El procedimiento de configuración es idéntico para ambos. Cuando se incluye un rol de seguridad en una regla de replicación, se debe además configurar una regla de replicación para replicar todos los privilegios del rol. El rol de seguridad replicado no reconoce ningún privilegio que ya existe en el equipo con Notification Server de destino.

Requisitos de replicación

Los requisitos para configurar la replicación en Notification System deben cumplirse antes de configurar cualquier replicación.

Los requisitos de replicación son los siguientes:

- El tráfico de red debe ser enrutable entre Notification Servers.
- El tráfico de HTTP/HTTPS debe estar permitido entre Notification Servers.
- Deben existir relaciones de confianza entre los Notification Servers o se deben conocer las credenciales de las cuentas privilegiadas que facilitan la confianza.
- Cada Notification Server debe poder determinar el nombre y la dirección de red de cualquier Notification Server con el que replica datos.
- Debe haber suficiente ancho de banda entre los Notification Servers para admitir la réplica de paquetes de soporte y de datos.

El hardware y el ancho de banda necesarios dependen del tamaño de la topología de la infraestructura y de los datos replicados.

- Cada Notification Server debe contar con un servidor de sitio que ejecute el servicio de administración de paquetes disponible. El servicio de administración de paquetes debe prestarse a Notification Server.

Ver "Acerca de la replicación y las reglas de replicación" en la página 172.

Configuración de las reglas de replicación

Antes de iniciar la replicación de datos de un Notification Server a otro, es necesario planear la replicación. Esto es para asegurarse de que los datos similares no pasen en ambas direcciones. Si cualquiera de los servidores forma parte de una jerarquía, debe asegurarse de que la replicación no entre en conflicto con el proceso de réplica de la jerarquía. Notification Server no verifica que la configuración de réplica sea coherente con la jerarquía. Una implementación mal planeada podría crear conflictos entre los datos o sobrescritura de datos en las CMDB afectadas.

Ver "Acerca de la replicación y las reglas de replicación" en la página 172.

Ver "Requisitos de replicación" en la página 174.

La regla debe estar habilitada para que la réplica específica tenga lugar. Puede habilitar y deshabilitar las reglas de replicación en cualquier momento, según las necesidades de la organización. Para que se habilite cada regla, los datos especificados se replican según la programación definida.

Puede replicar los datos en cualquier momento mediante la ejecución de las reglas de replicación correspondientes. En la consola, haga clic con el botón derecho en la regla y en **Ejecutar**. La ejecución de una regla de replicación sobrescribe su programación y replica los datos especificados en los servidores de destino de inmediato. La ejecución de una regla de replicación es una operación única que no cambia la programación de la réplica. Todas las reglas de replicación continúan ejecutándose según su programación.

Nota: La replicación no se admite entre dos Notification Servers que tienen diferentes versiones de IT Management Suite instaladas. Por ejemplo, no se puede replicar datos de un servidor 7.0 a un servidor 7.1.

Para configurar una regla de replicación

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Todas las configuraciones**.
2. En el panel izquierdo, expanda la carpeta **Configuración > Notification Server > Replicación**.
3. En la carpeta **Replicación**, realice una de las acciones siguientes:

Cree una nueva regla de replicación	Haga clic con el botón derecho en la carpeta apropiada y haga clic en **Nuevo > Regla de replicación**. La regla nueva aparece en la carpeta y se selecciona automáticamente.
Modifique una regla de replicación existente	Expanda la carpeta apropiada y luego seleccione la regla de replicación que desee modificar.
Habilite o deshabilite una regla de replicación	Expanda la carpeta apropiada y, a continuación, haga clic con el botón derecho en la regla de replicación y en **Habilitar** o **Deshabilitar**, según corresponda. También puede habilitar o deshabilitar las reglas en la página **Regla de replicación**. Para ello, haga clic en el icono de estado de la regla (Activada o Desactivada) para cambiar el valor.
Ejecute una regla de replicación	Expanda la carpeta apropiada y, a continuación, haga clic con el botón derecho en la regla de replicación que desee ejecutar y en **Ejecutar**.

4. En la página **Regla de replicación**, especifique las opciones apropiadas.

   Para obtener más información, haga clic en la página y después presione **F1**.
5. Haga clic en **Guardar cambios**.

Capítulo 10

Cómo realizar una configuración por primera vez

En este capítulo se incluyen los temas siguientes:

- Cómo realizar las tareas de configuración por primera vez

Cómo realizar las tareas de configuración por primera vez

Cuando instala Symantec Management Platform, configura Notification Server como parte del proceso de instalación. No se necesitan más configuraciones para comenzar a usar Notification Server.

En el caso poco probable de que se instale Symantec Management Platform sin las versiones que acompañan a ciertos productos, se muestran varios vínculos a las páginas de configuración. En esta situación, es necesario configurar la plataforma manualmente.

Ver "Acerca de configurar Notification Server" en la página 67.

Sin embargo, cuando se instala Symantec Management Platform y las versiones que acompañan a ciertos productos, se ve una página de portal **Bienvenido a Symantec Management Console** que simplifica el proceso de la configuración inicial.

Se ve la página **Bienvenido a Symantec Management Console** si se instala cualquiera de los siguientes productos:

- IT Management Suite

- Server Management Suite
- Client Management Suite

Algunas de las soluciones incluidas en el conjunto de aplicaciones quizá deban configurarse antes de utilizarlas. La página del portal de **Bienvenido a Symantec Management Console** es una único punto de entrada para realizar las acciones de configuración clave para las soluciones en los conjuntos que se han instalado. Estas acciones representan la configuración esencial que se debe definir para comenzar a usar las soluciones.

Una vez que se completa la configuración por primera vez, es posible que sea necesario realizar tareas de configuración adicionales. La necesidad de realizar pasos adicionales depende de las soluciones y de los conjuntos de aplicaciones que se han instalado inicialmente o que se instalan una vez que finaliza la configuración por primera vez. Existen otras opciones de configuración avanzadas disponibles en el menú **Configuración**, que pueden estar disponible en otras áreas de soluciones individuales.

Para obtener más información sobre las opciones de configuración para soluciones y productos individuales, consulte la documentación de esos productos.

Tabla 10-1 Proceso para realizar las tareas de configuración por primera vez

Paso	Tarea	Descripción
Paso 1	Detectar equipos.	Es necesario importar o detectar los equipos que están en su entorno. Ver "Detección de equipos" en la página 179.
Paso 2	Inicie Symantec Management Agent y los complementos de la solución.	Una vez que se detectan los equipos en su entorno, inicie Symantec Management Agent y los complementos de la solución en los equipos que desee administrar. Ver "Iniciar Symantec Management Agent y los complementos de la solución" en la página 181.
Paso 3	Recopilar inventario.	En este paso, Notification Server recopila la información que los agentes recién implementados reúnen de los equipos administrados. Ver "Recopilación de información de inventario" en la página 185.
Paso 4	Programe la administración de parches.	En este paso, se pueden programar la descarga y la instalación de las actualizaciones de software. Ver "Programación de la administración de parches" en la página 187.

Detección de equipos

Detectar los equipos significa identificar los equipos que están en su entorno. Antes de que pueda administrar los equipos, se debe primero identificar los equipos y seleccionar los que se deseen administrar usando Symantec Management Agent.

Para detectar los equipos, usted primero selecciona el tipo de equipos en los cuales se desee instalar Symantec Management Agent. Se detectan los equipos Windows con Importación de Active Directory. Se detectan equipos UNIX, Linux y Mac con un barrido de ping para un intervalo de IP que se selecciona.

Esta tarea es un paso en el proceso para realizar las tareas de configuración por primera vez.

Ver "Cómo realizar las tareas de configuración por primera vez" en la página 177.

Para detectar equipos

1. En Symantec Management Console, haga clic en **Inicio > Administración de Notification Server > Configuración por primera vez**.
2. En la página **Bienvenido a Symantec Management Console**, haga clic en **Detectar equipos**.
3. En el asistente **Detectar equipos**, realice los pasos siguientes:

Paso 1. Windows Le permite importar los equipos Windows por dominio o por grupo de trabajo.

Nota: Si prefiere detectar los equipos usando un análisis de red, no seleccione nada en esta página, pero haga clic en **Siguiente**.

Para importar los equipos Windows por dominio:

1. Seleccione el cuadro para importar los equipos Windows.
2. Haga clic en una casilla de verificación para elegir si importar de Microsoft Active Directory o a través de la pertenencia a dominio o WINS.
3. Haga clic en la flecha hacia abajo al lado de **Dominio o grupo de trabajo** para seleccionar un dominio o un grupo de trabajo. O se puede escribir un nombre de dominio o un nombre del grupo de trabajo manualmente.
4. Escriba las credenciales del dominio.
5. Haga clic en la opción al lado de **Programar importación recurrente** a la posición **Activado** o **Desactivado**.

   Si espera agregar nuevos equipos a su red, deje esta configuración activada. Dejar esta configuración activada significa que a medida que se agreguen los equipos a su red, serán detectados de forma automática.
6. Haga clic en **Programación**.

   Seleccione una programación compartida preestablecida para la importación recurrente. Esta lista se completa desde la página **Programaciones compartidas**. Se modifican, crean y usan las programaciones compartidas en **Configuración > Notification Server > Programaciones compartidas**.
7. Haga clic en **Siguiente**.

Paso 2. Red

Le permite detectar los equipos usando un análisis de red (barrido de ping).

Nota: Si prefiere importar los equipos Windows por dominio o grupo de trabajo, no seleccione nada en esta página, pero haga clic en **Atrás**.

Para detectar los equipos usando un análisis de red:

1. Seleccione el cuadro para detectar los equipos y los dispositivos en red.
2. Escriba un intervalo de barrido de ping.

   Considere si es necesario analizar todas las direcciones IP. Para una configuración por primera vez, es posible que sea necesario incluir todas las subredes para asegurarse de que se identifique cada dispositivo. Sin embargo, se puede limitar el alcance según las necesidades. Por ejemplo, se pueden ejecutar varios análisis en subredes específicas si eso simplifica la tarea de detección.
3. Si desea comunicarse con los dispositivos de red y clasificarlos más exactamente, haga clic en **Activar intervalos adicionales**.

   Nota: Si no se puede conectar remotamente, su red o equipos pueden tener firewalls activados. Es posible que sea necesario desactivarlos para realizar la detección.
4. Si desea continuar de forma inmediata al paso de configuración de la segunda configuración por primera vez, seleccione **Ejecutar Asistente de agente de distribución de Symantec**.

   Ver "Iniciar Symantec Management Agent y los complementos de la solución" en la página 181.

4. Haga clic en **Detectar**.

Iniciar Symantec Management Agent y los complementos de la solución

El asistente **Realizar instalación distribuida del agente** le permite iniciar Symantec Management Agent y los complementos de la solución en los equipos que desee administrar. Además le permite optimizar la distribución del agente según el número de equipos en su entorno.

Una vez que Symantec Management Agent está instalado en un equipo cliente, el agente envía una solicitud de registro a Notification Server para establecer la comunicación de confianza. De acuerdo con las reglas que se especifican en las políticas de registro de agentes, Notification Server de forma automática permite o bloquea las solicitudes de registro. Tenga en cuenta que la política de registro de agentes predeterminada acepta todas las solicitudes entrantes. Si desea permitir solamente al equipo especificado que se registre de forma automática en su Notification Server, defina políticas de registro de agentes personalizadas.

Ver "Acerca del registro de agente" en la página 237.

Ver "Crear una política de registro de agente" en la página 243.

Es posible comprobar y administrar las solicitudes de registro en la página **Estado de registro del agente**, en **Informes > Administración de Notification Server > Registro**.

Ver "Ver y administrar el estado de registro del agente" en la página 251.

Esta tarea es un paso en el proceso para realizar las tareas de configuración por primera vez.

Ver "Cómo realizar las tareas de configuración por primera vez" en la página 177.

Para iniciar Symantec Management Agent y los complementos de la solución

1. En Symantec Management Console, haga clic en **Inicio > Administración de Notification Server > Configuración por primera vez**.
2. En la página **Bienvenido a Symantec Management Console**, haga clic en **Realizar instalación distribuida del agente**.

3 En el asistente **Realizar instalación distribuida del agente**, en el panel **Paso 1: Equipos**, seleccione los equipos en los cuales desee instalar el agente y después haga clic en **Siguiente**.

Instalar automáticamente en todos los equipos detectados	Le permite instalar el agente en todos los equipos detectados. Esta opción de instalación además le permite seleccionar una programación de instalación recurrente de una lista desplegable. Esta lista se completa desde la página **Programaciones compartidas**. Se modifican, crean y usan las programaciones compartidas en **Configuración > Notification Server > Programaciones compartidas**.
Solamente en equipos detectados seleccionados	Le permite escribir el nombre de equipos o buscar equipos específicos en los cuales instalar el agente. Esta opción presenta una lista típica de selección. La columna izquierda, que se conoce como la columna de la detección, le permite buscar o seleccionar en una lista de equipos detectados. La columna derecha, que se conoce como la columna de seleccionados, muestra una lista de equipos seleccionados de la columna de la detección. En la columna de detección, escriba todo o una parte de un nombre de equipo. Puede también usar criterios de búsqueda, tales como XP, Win u otras letras que un grupo de sus nombres de equipo preferidos contiene. La columna de detección enumera los equipos detectados que coinciden con sus criterios de búsqueda. Use las teclas de flecha para mover los equipos de la columna de detección a la columna seleccionada. A medida que traslada equipos a la columna seleccionada, se ve el número de equipos seleccionados cambiar en la parte inferior derecha de la columna. Esta opción de instalación además le permite agregar criterios de búsqueda para los equipos detectados seleccionados. Es posible restringir los resultados en la columna seleccionada buscando los equipos por nombre o dirección IP.

4 En el panel **Paso 2: Complementos**, seleccione los complementos que desee instalar y después haga clic en **Siguiente**.

Seleccione los complementos para todas las soluciones que se han instalado. Además se deben seleccionar los complementos según las funciones de administración que desea realizar. Por ejemplo, si desea recopilar el inventario, asegúrese de que los complementos de Inventory que son relevantes para su entorno estén activados.

Activar todas	Le permite activar todos los complementos que se detallan. Cuando se activan todos los complementos, se ve un sombreado verde a lo largo del lado izquierdo de la lista. Cuando se desactivan todos los complementos, se ve un sombreado rojo.
Barra **Encendido/Apagado**	Le permite encender o apagar complementos seleccionados. El sombreado rojo o verde indica qué complementos están apagados (rojo) y qué complementos están encendidos (verde).

5 En el panel **Paso 3: Optimizar**, seleccione el entorno de la distribución:

Entorno de producción	Le permite optimizar la distribución del agente según el número de equipos en su entorno de producción. El número de equipos en su entorno determina los intervalos óptimos para descargar la configuración del agente y comprobar la existencia de nuevas tareas. Cuando se selecciona el número de equipos con el control deslizante, el asistente de forma automática ajusta esos intervalos. Ver "Opciones de configuración de agente y tareas" en la página 184. Para consultar los detalles de la configuración del agente y de la configuración de la tarea, haga clic en **Mostrar detalles** y después haga clic en **Aceptar**.
Entorno de prueba (1 a 50 equipos)	Le permite probar la instalación distribuida en un subconjunto de equipos instalados.

6 Haga clic en **Realizar instalación distribuida del agente**.

Opciones de configuración de agente y tareas

En el asistente **Realizar instalación distribuida del agente**, se ve un control deslizante que le permite seleccionar de 0 a más de 15 000 equipos. De acuerdo

con el número de equipos que se selecciona, el asistente ajusta automáticamente su sistema para optimizar el rendimiento.

Haga clic en **Mostrar detalles** para consultar la configuración optimizada. El cuadro de diálogo **Configuración optimizada** muestra cuántas veces una nueva configuración se descarga para la configuración del agente. Además enumera el tiempo máximo entre los intentos de mandar una señal para la configuración de la tarea.

Los detalles en el asistente se aplican a los equipos detectados en los cuales usted elige instalar el agente. Si es necesario configurar o modificar las opciones de configuración del agente para otros equipos, se puede hacer en Symantec Management Console, en **Configuración > Agentes/complementos > Configuración del agente de destino**. Para optimizar la configuración de la tarea, haga clic en **Configuración > Notification Server > Configuración del servidor de sitio** y, a continuación, en el panel izquierdo, haga clic en **Administración del sitio > Configuración > Task Service > Configuración de Task Service**. En el panel derecho, configure **Período mínimo entre intentos de envío de señales**.

Ver "Iniciar Symantec Management Agent y los complementos de la solución" en la página 181.

Tabla 10-2 Opciones para la configuración óptima de agente y tareas

Número de equipos en el entorno de producción	Configuración optimizada del agente	Configuración optimizada de la tarea
0 - 100	5 minutos.	1 minuto
100 - 5000	un hora	5 minutos
5000 - 10000	dos horas	5 minutos.
10000 - 15000	tres horas	5 minutos
15000 +	cuatro horas	5 minutos.

Recopilación de información de inventario

Recopilar la información inicial del inventario es clave para administrar su red. Todas las soluciones usan inventarios y la información que el inventario recopila completa las vistas de equipo, de software y otras páginas y campos en la consola. Saber qué está instalado en su red es crítico para recopilar los datos correctos de modo que se puedan tomar decisiones esenciales para la administración.

Su red es única. Por lo tanto, es necesario determinar qué información usted quiere recopilar, sobre qué recursos usted quiere recopilar información y cuántas veces se debe recopilar información.

En la ventana de la política **Recopilar el inventario** se puede desactivar la política o activar la política. Además seleccione una programación predeterminada o una programación personalizada en las cuales desee asegurarse de que la política sea actual. Antes de recopilar la información del inventario, considere de qué información es necesario realizar un seguimiento y cuántas veces usted quiere actualizar esa información. Se debe además considerar si existe alguna circunstancia en la cual se querría desactivar la política del inventario. La opción predeterminada es dejar la política activada.

Es posible recopilar los siguientes tipos de información del inventario:

Hardware y sistema operativo	Le permite recopilar el inventario de CPU, de discos duros, de memoria, de firmware, de usuarios y de grupos.
Software	Le permite recopilar el inventario sobre los paquetes de software de UNIX/Linux/Mac y los programas de Windows.
Propiedades de archivo	Le permite recopilar la información sobre fabricantes, versiones, tamaño y nombre interno.
Aplicaciones de servidor	Si tiene Inventory Pack instalado, le permite recopilar información sobre aplicaciones de servidor.

Esta tarea es un paso en el proceso para realizar las tareas de configuración por primera vez.

Ver "Cómo realizar las tareas de configuración por primera vez" en la página 177.

Para recopilar información del inventario

1. En Symantec Management Console, haga clic en **Inicio > Administración de Notification Server > Configuración por primera vez**.
2. En la página **Bienvenido a Symantec Management Console**, haga clic en **Recopilar inventario**.
3. En la ventana de la política **Recopilar inventario completo** al lado de **Políticas o acciones de política**, deje la política activada.

   Si tiene una necesidad determinada de detener la ejecución de la política por un período, haga clic en **Desactivar** para desactivar la política.
4. Seleccione una programación para mantener la política actual. Es posible seleccionar una programación predeterminada o crear una programación personalizada.

   Esta lista de programaciones se completa desde la página **Programaciones compartidas**. Se modifican, crean y usan las programaciones compartidas en **Configuración > Notification Server > Programaciones compartidas**.

5 En la ventana de la política **Recopilar inventario completo**, revise los detalles del inventario y seleccione los tipos de inventario para recolectar. Realice los cambios según sea necesario.

Para consultar los detalles sobre los tipos de inventario que usted seleccionó, en el área **Políticas o acciones de política** de la ventana haga clic en **Avanzado**. Es posible seleccionar los elementos adicionales sobre los cuales desee recopilar datos de inventario. Si realiza cambios, haga clic en **Aceptar**.

6 En la ventana de la política **Recopilar inventario completo** en el área **Se aplica a/Cumplimiento**, revise los detalles.

Esta área muestra los detalles sobre el inventario que se recopila en los equipos de destino. Es posible verificar el cumplimiento de la política del inventario, modificar los equipos que recopilan el inventario y realizar otros cambios según las necesidades.

7 Haga clic en **Guardar cambios**.

Programación de la administración de parches

El asistente **Programar parche** le permite especificar cuándo descargar las definiciones de actualización de software, cuántas veces analizar los equipos para las actualizaciones disponibles y cuándo instalar las actualizaciones. Es posible también especificar las notificaciones que desee recibir.

Esta tarea es un paso en el proceso para realizar las tareas de configuración por primera vez.

Ver "Cómo realizar las tareas de configuración por primera vez" en la página 177.

Para programar la administración de parches

1 En Symantec Management Console, haga clic en **Inicio > Administración de Notification Server > Configuración por primera vez**.

2 En la página **Bienvenido a Symantec Management Console**, haga clic en **Programar parche**.

3 En el asistente **Programar parche**, realice los pasos siguientes:

Paso 1: Descargar	Le permite especificar la programación de la descarga de las definiciones de actualización de software. Tenga en cuenta que si se activa la descarga de las definiciones de actualización de software para un sistema operativo, todos los distribuidores para este sistema operativo son seleccionados de forma automática para la descarga.
Paso 2: Notificaciones	Le permite especificar las notificaciones que desee recibir.
Paso 3: Analizar e instalar actualizaciones	Le permite especificar cuántas veces analizar los equipos para buscar las actualizaciones disponibles y cuándo instalar las actualizaciones.

4 Haga clic en **Programar parche**.

Sección 3

Detectar los recursos en su red

- Capítulo 11. Detección de equipos con Windows
- Capítulo 12. Importación de recursos de Active Directory
- Capítulo 13. Detección de dispositivos de red

Capítulo 11

Detección de equipos con Windows

En este capítulo se incluyen los temas siguientes:

- Métodos de detección de recursos
- Métodos de detección para equipos Windows
- Cómo detectar equipos con la detección de recursos de dominio

Métodos de detección de recursos

La detección de todos los recursos en su red es uno de los primeros pasos para la correcta administración de su red. Symantec Management Platform proporciona herramientas para detectar dispositivos en su red de forma automática. También crea recursos para aquellos dispositivos detectados en la base de datos de administración de configuración, también conocida como CMDB. La posibilidad de detectar recursos de forma automática evita pérdida de tiempo y aparición de errores debido a la entrada manual.

Puede ejecutar una detección manual en cualquier momento o puede configurar una programación. Al programar una detección, puede crear de forma automática recursos de la CMDB para equipos nuevos a medida que estos se agregan a la red.

Tabla 11-1 Métodos de detección de recursos

Método	Descripción
Detección de recursos de dominio	Si desea detectar equipos Windows de manera rápida, puede utilizar la detección de recursos de dominio. Este método le permite detectar los equipos que cuentan con una cuenta de confianza en el dominio. Cuando instaló Notification Server, tuvo la oportunidad de utilizar este método para detectar equipos de forma automática. Ver "Métodos de detección para equipos Windows" en la página 191.
Importación de Active Directory	Puede importar algunos o todos los recursos en su Microsoft Active Directory dentro de la CMDB. Puede configurar reglas de importación de recursos para identificar e importar los recursos que desee. Luego, puede configurar programaciones para realizar importaciones completas e importaciones de actualización en los intervalos apropiados. Ver "Métodos de detección para equipos Windows" en la página 191.
Network Discovery	Si desea detectar todos los recursos en todas las plataformas, utilice Network Discovery. Al utilizar Network Discovery, puede detectar todos los dispositivos IP que están conectados en la red. Puede detectar enrutadores, conmutadores, concentradores, impresoras de red, servidores Novell NetWare, equipos Windows, UNIX, Linux y Macintosh. Ver "Acerca de Network Discovery" en la página 208.

Métodos de detección para equipos Windows

Antes de que administre sus equipos, debe hacer lo siguiente:

- Detectar los equipos en la red.
- Crear recursos para estos equipos en CMDB

Este proceso se denomina detección y permite detectar los equipos en los cuales se puede instalar Symantec Management Agent y varios agentes y complementos de la solución.

Para detectar equipos Windows, haga lo siguiente:

- Buscar todos los equipos Windows en su red que están registrados en un dominio específico.
- Buscar todos los equipos Windows en su red que coincidan con las unidades organizativas que especifica.

Si desea detectar los equipos que se están ejecutando con otros sistemas operativos, puede utilizar Network Discovery.

Ver "Métodos de detección de recursos" en la página 190.

Tabla 11-2 Métodos de detección para equipos Windows

Método	Descripción
Descubrimiento de recursos	Busca el dominio especificado para todos los equipos que se registren en ese dominio. Es necesario elegir por lo menos uno de la Lista de exploración de dominios o de las opciones Pertenencia al dominio. Ver "Cómo detectar equipos con la detección de recursos de dominio" en la página 192.
Importación de Microsoft Active Directory	Permite importar los recursos del equipo que coinciden con las unidades organizativas que se especifican. Es posible también filtrar los equipos que han sido activos dentro de un número específico de días o que ejecutan un sistema operativo específico de Windows. Este método arroja información detallada de los sistemas operativos para cada uno de sus equipos detectados y es el método preferido. Ver "Importación de recursos mediante la importación de Microsoft Active Directory" en la página 199.

Puede utilizar estos métodos de detección para detectar todos sus equipos en dominios o puede concentrarse en equipos en un solo dominio.

Cómo detectar equipos con la detección de recursos de dominio

Puede detectar equipos Windows buscando información sobre recursos de dominio. Los equipos detectados tienen un recurso creado para ellos en CMDB. Puede ejecutar una detección de forma manual o mediante una programación. Tras la ejecución de una detección, puede ver los informes que muestran los resultados de dicha detección.

Esta base de datos contiene la siguiente información de cada equipo detectado:

- Nombre (lista de exploración de dominios y pertenencia al dominio)

- Nombre de sistema operativo (lista de exploración de dominios y pertenencia al dominio)
- Versión principal (lista de exploración de dominios)
- Versión secundaria (lista de exploración de dominios)
- Plataforma (lista de exploración de dominios)

Ver "Métodos de detección para equipos Windows" en la página 191.

Nota: El mensaje de estado en la página **Detección de recursos** muestra la última vez que la detección se realizó de forma manual a partir de la página. La hora no se actualiza para mostrar cualquier detección programada que se haya ejecutado posteriormente.

Para detectar equipos con la detección de recursos de dominio

1. En Symantec Management Console, en el menú **Acciones**, haga clic en **Detectar** > **Importar pertenencia a dominio o WINS**.
2. En la página **Importación de pertenencia a dominio o WINS**, en **Dominios para buscar**, escriba el nombre de un dominio que desee buscar y a continuación haga clic en el icono Agregar.
3. (Opcional) Para escribir un nombre de usuario y una contraseña diferentes para el dominio de modo que Notification Server tenga acceso, complete los siguientes pasos:
   - Seleccione el dominio.
   - Haga clic en el icono en forma de lápiz.
   - Haga clic en **Usar estas credenciales**.
   - Escriba el nombre de usuario y la contraseña y, luego, haga clic en **Aceptar**.
4. Seleccione por lo menos una de las siguientes opciones:

Lista de exploración de dominios

Este método se diseña para los entornos pequeños, de punto a punto.

El método usa la lista de exploración de red para detectar todos los equipos en el dominio. La opción Examinar detecta todos los equipos que comparten archivos o impresoras, o que están ejecutando el servicio Windows Messenger. Estos incluyen equipos con Windows NT, 2000, 2003, 2008, 95, 98, 98 SE, ME, XP, 7 y 8.

Este método también puede detectar equipos en un grupo de trabajo que concuerde con el criterio de búsqueda.

La lista de exploración de dominios funciona enumerando los registros en la lista de exploración del equipo. La lista de exploración fue diseñada para un entorno pequeño, de punto a punto, de forma que no se escala bien en entornos grandes.

Cuando Notification Server realiza una detección de listas para examinar dominios, precisa una copia de la lista de examinación del equipo. La lista de examinación incluye información adicional, como el sistema operativo del equipo y su versión. A continuación, lleva a cabo una búsqueda inversa del nombre del equipo para obtener su dirección IP.

Podría experimentar problemas al detectar equipos utilizando este método si existe la siguiente condición:

- El equipo no está en la lista de exploración del equipo.
- El equipo está en la lista de exploración del equipo, pero se registra como archivos compartidos.
- Puede tomar entre 15 minutos y 51 minutos para que los cambios se reflejen en la lista de exploración del equipo.

El método de detección de listas para examinar dominios obtiene la información necesaria de la lista de exploración del equipo lo más rápidamente posible. Este método puede sobrecargar un PDC en un dominio grande o en un entorno de varios dominios. Symantec recomienda ejecutar este método fuera del horario de oficina, preferiblemente durante el fin de semana.

Pertenencia a dominio Esta opción detecta todos los equipos con cuentas de confianza en el dominio. Puede detectar equipos en dominios Windows NT 4.0 o Windows 2000, y en dominios posteriores de Active Directory. Este método encuentra todos los equipos con Windows NT, 2000, 2003, 2008, XP, 7 y 8 del dominio. Sin embargo, no se encuentra ningún equipo con Windows 95, 98, 98 SE y ME.

Nota: Se puede detectar información limitada en equipos en dominios NT 4.0. Por ejemplo, se desconoce el sistema operativo específico del equipo.

La detección de la pertenencia al dominio enumera las cuentas de equipos de los dominios especificados.

Cuando se agrega un equipo con Windows NT, 2000, 2003, 2008, XP, 7 y 8 a un dominio, se crea una cuenta de equipo en ese dominio. El equipo utiliza esta cuenta para autenticarse en el dominio, de manera que el equipo puede autenticar inicios de sesión de usuario por medio de una conexión segura. Los equipos con Windows 9x no crean una cuenta de equipo y por esta razón no se pueden encontrar con este método.

Al detectar equipos con el método de pertenencia al dominio, Notification Server cataloga estas cuentas. A diferencia del método de lista de exploración de dominios, estas cuentas no tienen información adicional que no sea el nombre del equipo. Notification Server aún hace una operación de búsqueda reversa del nombre para conseguir la dirección IP.

5 Elija alguna de las siguientes opciones:

Detectar ahora	Haga clic en **Detectar ahora**.
Configurar programación	En **Opciones de programación**, en la lista desplegable **Programación**, especifique la programación de la importación.

6 Haga clic en **Guardar cambios**.

7 Para ver los resultados de la detección, haga lo siguiente:

- Haga clic en **Ver informes de detección**.
- En la ventana **Informes sobre detección de recursos**, haga clic con el botón derecho en un informe y haga clic en **Abrir en una nueva ventana**.
- Escriba los parámetros para el informe.

- Haga clic en **Actualizar**.

Capítulo 12

Importación de recursos de Active Directory

En este capítulo se incluyen los temas siguientes:

- Acerca de la importación de Microsoft Active Directory
- Acerca de la importación de asociaciones de recursos
- Importación de recursos mediante la importación de Microsoft Active Directory

Acerca de la importación de Microsoft Active Directory

La función Importación de Microsoft Active Directory de la Plataforma de administración Symantec permite importar objetos de Active Directory, como usuarios, equipos, sitios y subredes, en la CMDB. Esta función permite aprovechar los datos que ya existen en Active Directory sin tener que volver a crearlos. Es posible programar importaciones regulares para mantener su CMDB completa con los recursos actualizados, lo que permite una mejor administración de su entorno.

La importación de Microsoft Active Directory usa el protocolo ligero de acceso a directorios (LDAP) para proporcionar una sincronización unidireccional de Active Directory a la Plataforma de administración Symantec. LDAP es el mismo protocolo usado por las herramientas estándares de administración de Active Directory. La importación de Microsoft Active Directory es compatible con Windows 2000, 2003 y 2008.

Para usar la importación de Microsoft Active Directory, es necesario definir las reglas apropiadas de importación de recursos para importar los recursos que desea. Es posible programar las reglas de importación de recursos para que se ejecuten en intervalos regulares y las puede ejecutar manualmente en cualquier momento.

Cuando se ejecuta una regla de importación de recursos, se pueden importar todos los datos apropiados (una importación completa). Alternativamente, se pueden importar los datos que son nuevos o están modificados en Active Directory desde la última importación (una importación de actualización). Como parte del proceso de importación, pueden crear automáticamente los filtros o los grupos organizativos en función de las unidades organizativas, los grupos de seguridad y los grupos de distribución que se configuran en Active Directory. Estos filtros se pueden usar para especificar los destinos de recursos a los cuales se aplican directivas y tareas.

Ver "Acerca de los filtros de recursos" en la página 353.

Ver "Importación de recursos mediante la importación de Microsoft Active Directory" en la página 199.

Durante el proceso de importación, los equipos de Active Directory se coinciden con los equipos administrados en la CMDB, usando el nombre y el dominio del equipo. Sin embargo, la importación de Microsoft Active Directory importa todos los equipos que las reglas de importación de recursos identifican, independientemente del estado de la instalación de Symantec Management Agent. La importación de todos los equipos permite importar los equipos nuevos y no administrados, y después destinar esos equipos a la instalación de Symantec Management Agent.

Nota: Es posible también detectar los equipos Windows nuevos y no administrados usando el descubrimiento de recursos.

Ver "Métodos de detección para equipos Windows" en la página 191.

Si hay algunos errores en el proceso de importación, se puede comprobar el registro de estado de la Plataforma de administración Symantec para obtener información. El registro de estado se puede acceder desde el menú Inicio en el equipo de la Plataforma de administración Symantec: **Todos los programas > Symantec > Diagnóstico > Altiris Log Viewer**.

La Plataforma de administración Symantec incluye un número de informes que proporcionan información en las actividades de importación de Microsoft Active Directory. Estos informes se almacenan en la carpeta **Informes > Administración de Notification Server > Microsoft Active Directory**.

Acerca de la importación de asociaciones de recursos

Microsoft Active Directory no solo almacena objetos, también almacena relaciones entre objetos. La importación de Microsoft Active Directory puede extraer estas relaciones de Active Directory y crear recursos apropiados y asociaciones del recurso en la CMDB. La importación de Microsoft Active Directory admite cuatro

asociaciones de recursos para usuarios y una asociación de recursos entre subredes y sitios.

Tabla 12-1 Asociaciones de recursos compatibles con la importación de Microsoft Active Directory

Asociación de recursos	Descripción
Usuario, compañía	Crea un recurso de compañía para el usuario importado según su atributo de “compañía” en Active Directory.
Usuario, departamento	Crea un recurso de departamento para el usuario importado según su atributo de “departamento” en Active Directory.
Usuario, usuario	Crea uno o más recursos de usuario para el usuario importado según su atributo de “directReports” en Active Directory.
Usuario, usuario	Crea un recurso de usuario para el usuario importado según su atributo de “administrador” en Active Directory.
Sitio, subred	Crea uno o más recursos de subred para el sitio importado según su atributo de “siteObjectBL” en Active Directory.
Subred, sitio	Crea un recurso de sitio para la subred importada según su atributo de “siteObject” en Active Directory.

La ventana **Activar asociaciones de recursos** permite usar estas relaciones en una regla de importación de recursos para importar otros recursos relacionados que no se especifiquen explícitamente en la regla. De forma predeterminada, se habilitan todas las asociaciones del recurso.

Ver "Creación y modificación de reglas de importación de recursos" en la página 201.

Importación de recursos mediante la importación de Microsoft Active Directory

Es posible importar todos los equipos registrados en Active Directory. Como alternativa, es posible importar solamente los equipos que coinciden con los criterios especificados por el usuario.

Ver "Acerca de la importación de Microsoft Active Directory" en la página 197.

Cuando se instala Symantec Management Platform, es posible usar la importación de Microsoft Active Directory para importar todos los equipos. Es posible destinar los equipos no administrados a la instalación de Symantec Management Agent. La importación de Microsoft Active Directory es el método preferido para identificar

equipos nuevos y no administrados. Devuelve información detallada sobre los sistemas operativos para cada uno de los equipos detectados.

Puede también usar Importación de Microsoft Active Directory para crear cuentas y roles de Symantec Management Platform de los usuarios y los grupos de Windows. Se importan los usuarios y los grupos de Windows, de modo que no tenga que crear manualmente las cuentas y los roles de Symantec Management Platform. Importación de Microsoft Active Directory tiene una regla de importación de recursos para importar recursos de rol y cuenta. Cuando esta regla se ejecuta, se duplica la estructura de usuarios y grupos de Windows en Symantec Management Platform. Crea una cuenta de Symantec Management Platform para todos los usuarios de Windows en los grupos de seguridad seleccionados. Además crea los roles de Symantec Management Platform para cada uno de los grupos de seguridad seleccionados. Finalmente, coloca las cuentas de administración de Symantec creadas recientemente en los roles de Symantec Management Platform donde se pone al usuario correspondiente de Windows en el grupo correspondiente de Windows.

Después de realizar la importación inicial, es posible configurar las reglas de importación de recursos que comprueban regularmente Active Directory para detectar recursos nuevos o modificados e importar los recursos apropiados a la CMDB.

Una vez que se configuran las reglas de importación de recursos, es posible especificar la estructura de origen de Active Directory desde la cual se realizan las importaciones. Es posible aplicar las restricciones que filtran los equipos importados según los requisitos del usuario. Por ejemplo, es posible importar solamente los equipos que han cambiado la contraseña de cuenta de equipo durante una cantidad de días determinada o los equipos que se encuentran ejecutando un sistema operativo de Windows determinado.

Tabla 12-2 Proceso para importar recursos mediante la importación de Microsoft Active Directory

Paso	Acción	Descripción
Paso 1	Configure las reglas de importación de recursos adecuadas.	Puede crear todas las reglas de importación de recursos nuevas que desee y modificar las reglas existentes para que se adapten a sus requisitos. También puede eliminar las reglas que ya no necesite. Ver "Creación y modificación de reglas de importación de recursos" en la página 201.

Paso	Acción	Descripción
Paso 2	Programe las reglas de importación de recursos.	Para cada regla de importación de recursos, puede programar importaciones completas o importaciones de actualización para ejecutarlas en los intervalos adecuados. Ver "Programación de reglas de importación de recursos" en la página 204.
Paso 3	Configure la programación de Sincronización del directorio.	La programación de Sincronización del directorio identifica los recursos importados anteriormente que ya no existen en Active Directory y los elimina de la CMDB. Ver "Cómo configurar la programación de sincronización del directorio" en la página 205.
Paso 4	(Opcional) Ejecute una regla de importación de recursos manualmente.	Puede ejecutar una regla de importación de recursos manualmente en cualquier momento. Puede ejecutarla como una importación completa o una importación de actualización. Ver "Ejecución manual de reglas de importación de recursos" en la página 206.

Creación y modificación de reglas de importación de recursos

Las reglas de importación de recursos le permiten especificar los recursos que desea importar desde Active Directory.

Seis reglas predeterminadas de importación de recurso se proporcionan con la Plataforma de administración Symantec, uno para cada uno de los tipos de recursos admitidos: Usuario, equipo, cola de impresión, sitio, subred, rol y cuenta. Es posible modificar estas reglas para adaptarse a sus requisitos o se pueden crear nuevas reglas para importar los recursos que desee.

Es posible configurar una regla para crear automáticamente los filtros o los grupos organizativos basados en las unidades organizativas de Active Directory, los grupos de seguridad y los grupos de distribución de los que la regla importa los recursos. Estos filtros se pueden entonces usar para especificar los destinos de recursos a los cuales se aplican directivas y tareas.

Es posible programar las reglas de importación de recursos para actualizar la CMDB en intervalos regulares o se puede ejecutar una regla determinada manualmente en cualquier momento. Ejecutar las reglas de importación de recursos periódicamente garantiza que cualquier cambio a Active Directory está reflejado en la CMDB.

Esta tarea es un paso en el proceso para importar recursos mediante la importación de Microsoft Active Directory.

Ver "Importación de recursos mediante la importación de Microsoft Active Directory" en la página 199.

Para crear o modificar una regla de importación de recursos

1 En Symantec Management Console, en el menú **Acciones**, haga clic en **Detectar > Importar Microsoft Active Directory**.

2 En la página **Importación de Microsoft Active Directory**, realice una de las siguientes tareas:

Para crear una regla de importación de recursos	En la barra de herramientas, haga clic en **Crear una nueva regla de importación**. La nueva regla se añade a la lista de reglas de importación de recursos.
Para modificar una regla existente de importación de recursos	En la lista de reglas de importación de recursos, seleccione la regla apropiada.
Para eliminar una regla de importación de recursos	En la lista de reglas de importación del recurso, selecciona la regla apropiada y, a continuación, en la barra de herramientas, haga clic en **Suprimir la regla de importación seleccionada**.

3 En la regla de importación de recursos que desee modificar, para cada uno de los vínculos resaltados, haga clic en el vínculo y después especifican la configuración apropiada.

Tipo de recurso especificado (configuración predeterminada), equipo, usuario, sitio, subred	Especifique el tipo de dominio y el tipo de recurso que desea importar y la estructura apropiada de origen de Active Directory.
Origen de datos especificado (configuración predeterminada)	Especifique el dominio o el servidor (controlador de dominio) y las credenciales apropiadas de la cuenta desde las cual desea importar recursos.

Ninguno (configuración predeterminada)	Cuando hace clic en este vínculo, aparece uno de los siguientes cuadros de diálogo: ■ **Seleccionar unidad organizativa (UO)** Seleccione las unidades organizativas o los contenedores de Active Directory (cualquiera que corresponda a la estructura de origen que especificó en la ventana **Selección de recursos**) desde la que se importarán los recursos. Cuando se selecciona una unidad organizativa o un contenedor, se puede elegir si se desean incluir a sus descendientes. ■ **Seleccionar grupos de seguridad** o **Seleccionar grupos de distribución** Seleccione los grupos determinados de Active Directory de los que desea importar usuarios y grupos. El cuadro de diálogo **Seleccionar grupos de seguridad** aparece solamente para la regla que importa a recursos de cuenta y roles.
Asignaciones de columnas específicas (configuración predeterminada), asignaciones de columnas predeterminadas	Especifique la asignación entre la CMDB de la Plataforma de administración Symantec y los campos de datos de recursos de Active Directory. Es posible usar estas asignaciones para importar atributos adicionales cuando se ha extendido el esquema de Active Directory.
Todos los equipos, **Todos los usuarios**	Especifique los criterios apropiados para restringir los recursos importados a solamente los que coincidan con los criterios especificados. Se importa un recurso solamente si cumple con todos los criterios especificados.
Estas asociaciones de recurso	Especifique las asociaciones de recurso que desee usar para importar otros recursos relacionados que no se especifiquen explícitamente en la regla de importación del recurso. De forma predeterminada, se habilitan todas las asociaciones del recurso. La importación de Microsoft Active Directory puede extraer estas relaciones de Active Directory y crear recursos apropiados y asociaciones del recurso en la CMDB. Ver "Acerca de la importación de asociaciones de recursos" en la página 198.

Programaciones específicas	Especifique las programaciones que se utilizan para importar recursos. Puede especificar las programaciones para importaciones de datos completas y actualizadas. Ver "Programación de reglas de importación de recursos" en la página 204.

4 Seleccione la casilla **Habilitada** apropiada para habilitar la importación de equipos, usuarios, subred y recursos de sitio.

5 Haga clic en **Aplicar**.

Programación de reglas de importación de recursos

Para cada regla de importación de recursos, es posible especificar las programaciones apropiadas para la importación completa y la importación de actualización. Una importación completa importa todos los recursos del dominio o del controlador de dominio de destino. Una importación de actualización importa solamente los recursos que han tenido modificaciones desde la última vez que se ejecutó la regla de importación de recursos.

Se puede establecer una sola regla de importación de recursos que incluya ambas programaciones o configurar reglas de importación diferentes para las importaciones completas y las importaciones de actualización. Si se establece una regla específica para la importación de actualización, se recomienda que la regla apunte a un controlador de dominio en lugar de un dominio.

Una importación de actualización se ejecuta como una importación completa si cualquiera de las siguientes condiciones es verdadera:

- La regla se ejecuta por primera vez.
- El dominio o el servidor que se especifican en la regla han cambiado.
- El controlador de dominio desde el cual la regla ejecutó la importación anteriormente no está disponible.

Si es necesario, es posible anular la programación y ejecutar una regla de importación de recursos manualmente en cualquier momento.

Ver "Creación y modificación de reglas de importación de recursos" en la página 201.

Ver "Ejecución manual de reglas de importación de recursos" en la página 206.

Esta tarea es un paso en el proceso para importar recursos mediante la importación de Microsoft Active Directory.

Ver "Importación de recursos mediante la importación de Microsoft Active Directory" en la página 199.

Para programar reglas de importación de recursos

1. En Symantec Management Console, en el menú **Acciones**, haga clic en **Detectar > Importar Microsoft Active Directory**.
2. En la página **Importación de Microsoft Active Directory**, junto a la regla de importación de recursos que desea programar, seleccione la opción **Habilitada**.
3. En la descripción de la regla de importación de recursos, haga clic en **Programaciones especificadas**.
4. En la ventana **Programación de reglas**, configure ambas o una de las siguientes programaciones:

Programación de importación completa	Importa todos los recursos que la regla de importación de recursos identifique.
Actualizar programación	Importa solamente los recursos nuevos y modificados que son identificados por la regla de importación de recursos.

   Ver "Para configurar una programación" en la página 205.
5. Haga clic en **Aceptar** para cerrar la página **Programación de reglas**.
6. Haga clic en **Aplicar**.

Para configurar una programación

1. En la programación apropiada, seleccione la opción **Habilitar**.
2. En la lista desplegable **Programación**, seleccione una de las siguientes programaciones:

En la fecha/hora	Especifique la fecha y hora apropiadas. Si desea que la programación se repita, seleccione **Repetir cada** y después especifique el intervalo de repetición.
Programación compartida	Seleccione la programación compartida apropiada.

Cómo configurar la programación de sincronización del directorio

Para mantener la CMDB sincronizada con los recursos de Active Directory, es necesario configurar la programación apropiada de sincronización del directorio. La programación de sincronización del directorio identifica cualquier recurso previamente importado que ya no exista en Active Directory y lo quita de la CMDB. Además detecta cualquier recurso al que se le haya cambiado el nombre o movido

fuera de las unidades organizativas de las cuales se importaron inicialmente, y elimina los registros correspondientes de la CMDB.

Advertencia: Si se mueve un equipo desde un dominio a un grupo de trabajo, deberá eliminar el registro del equipo de Active Directory para evitar la duplicación en la CMDB.

Esta tarea es un paso en el proceso para importar recursos mediante la importación de Microsoft Active Directory.

Ver "Importación de recursos mediante la importación de Microsoft Active Directory" en la página 199.

Para configurar la programación de la sincronización del directorio

1. En Symantec Management Console, en el menú **Acciones**, haga clic en **Detectar > Importar Microsoft Active Directory**.
2. En la página **Importación de Microsoft Active Directory**, en **Programación de sincronización del directorio**, seleccione **Habilitado**.
3. En la lista desplegable **Programación**, seleccione una de las siguientes programaciones:

En la fecha/hora	Especifique la fecha y hora apropiadas. Si desea que la programación se repita, seleccione **Repetir cada** y después especifique el intervalo de repetición.
Programación compartida	Seleccione la programación compartida apropiada.

4. Haga clic en **Aplicar**.

Ejecución manual de reglas de importación de recursos

Si es necesario importar los recursos determinados de forma inmediata, se puede ejecutar manualmente la regla apropiada de importación de recursos. Es posible ejecutar la regla de importación de recursos como una importación completa o una importación de actualización. Ejecutar manualmente una regla de importación de recursos no tiene ningún efecto en su programación, si se habilita una.

Ver "Programación de reglas de importación de recursos" en la página 204.

Esta tarea es un paso en el proceso para importar recursos mediante la importación de Microsoft Active Directory.

Ver "Importación de recursos mediante la importación de Microsoft Active Directory" en la página 199.

Para ejecutar reglas de importación de recursos manualmente

1. En Symantec Management Console, en el menú **Acciones**, haga clic en **Detectar > Importar Microsoft Active Directory**.
2. En la página **Importación de Microsoft Active Directory**, seleccione la regla de importación de recursos que desee ejecutar.
3. Haga clic en alguna de las siguientes opciones:

Ejecutar ahora la regla de importación seleccionada (importación completa)	Ejecuta una importación completa de la regla seleccionada de importación de recursos.
Ejecutar ahora la regla de importación seleccionada (importación de actualización)	Ejecuta una importación de actualización de la regla seleccionada de importación de recursos.

4. Si desea detener el proceso de importación por cualquier motivo, haga clic en **Detener**.

Capítulo 13

Detección de dispositivos de red

En este capítulo se incluyen los temas siguientes:

- Acerca de Network Discovery
- Detección de dispositivos de red
- Delegar tareas de Network Discovery a usuarios que no son administradores
- Importación de archivos MIB

Acerca de Network Discovery

Network Discovery permite detectar todos los dispositivos IP que se conecten a su red. Network Discovery permite encontrar nuevos dispositivos de red y encontrar dispositivos de red cuyas propiedades de detección hayan cambiado.

Network Discovery se incluye en Symantec Management Platform.

Network Discovery puede detectar enrutadores, conmutadores, concentradores, impresoras de red, servidores de Novell NetWare y equipos que ejecutan Windows, UNIX, Linux y Macintosh. Es posible usar una variedad de protocolos para detectar dispositivos, como AMT, SNMP, WMI y otros.

La información recopilada puede ayudarlo a hacer lo siguiente:

- Planificar la toma de imágenes
- Actualizar los controladores en tipos específicos de hardware
- Configurar las modificaciones en enrutadores o conmutadores
- Cómo identificar los equipos que están ejecutando los sistemas operativos que actualmente no son admitidos por Symantec Management Agent

Es posible también actualizar categorías para poder identificar nuevos dispositivos que se agregan a la red durante la detección.

Como Network Discovery se integra con Symantec Management Platform, cuando se detectan los dispositivos, se crean automáticamente como recursos en la base de datos central de la plataforma (CMDB). Mediante el componente de administración de tareas de la plataforma, se pueden programar tareas de detección para ejecutarlas cuando mejor satisfaga sus necesidades.

Ver "Detección de dispositivos de red" en la página 209.

Ver "Delegar tareas de Network Discovery a usuarios que no son administradores" en la página 221.

Es posible también detectar equipos basados en Windows mediante dominios o por medio de la importación mediante Microsoft Active Directory.

Ver "Métodos de detección de recursos" en la página 190.

Detección de dispositivos de red

A fin de ayudarlo a administrar la red de forma satisfactoria, debe identificar los diversos dispositivos de ella. Network Discovery permite buscar nuevos dispositivos en la red, identificar los dispositivos previamente detectados y que ya no se encuentren, y buscar dispositivos de red cuyas propiedades de detección hayan cambiado. La detección se realiza mediante la ejecución de tareas que detecte dispositivos e informe los datos al Notification Server. Los datos detectados en cuanto a los dispositivos se almacenan como recursos conocidos en la Base de datos de la administración de configuración (CMDB). A fin de mantener los datos de detección actualizados, configure las tareas de detección automatizadas para que se ejecuten a intervalos regulares.

Es posible detectar todos los dispositivos en su red e introducir esos dispositivos en la CMDB.

Ver "Acerca de Network Discovery" en la página 208.

Tabla 13-1 Proceso para detectar dispositivos de red

Paso	Acción	Descripción
Paso 1	(Opcional) Configure las opciones de Network Discovery.	Es posible configurar las opciones predeterminadas de la tarea y configurar las clasificaciones de SNMP. Ver "Cómo establecer la configuración de detección" en la página 210.

Paso	Acción	Descripción
Paso 2	Cree una tarea de Network Discovery.	Es posible crear y programar una tarea para detectar un único dispositivo o varios dispositivos en una red. Es posible usar dos métodos para crear tareas: usando el Asistente de Network Discovery o creando las tareas manualmente. Ver "Creación de tareas de Network Discovery con el asistente" en la página 212. Ver "Creación y modificación manual de tareas de Network Discovery" en la página 213.
Paso 3	(Opcional) Modifique la configuración o las programaciones de la tarea.	Una vez que se crea una tarea de Network Discovery, se puede modificar la configuración de la tarea o agregar programaciones adicionales. Ver "Creación y modificación manual de tareas de Network Discovery" en la página 213.
Paso 4	Visualice los datos de la detección.	Es posible ver el estado de las tareas de Network Discovery y visualizar informes que muestren los resultados de la detección. Ver "Visualización de dispositivos detectados en vistas organizativas" en la página 219. Ver "Visualización de informes de detección" en la página 219.
Paso 5	Clasifique los dispositivos desconocidos.	Si hay dispositivos de clasificación desconocida, modifique la lista de clasificaciones de SNMP. Ver "Clasificación de dispositivos SNMP " en la página 220.

Cómo establecer la configuración de detección

Puede configurar opciones globales para las tareas de Network Discovery. Dichas opciones se utilizan cuando se crea una tarea nueva.

Es posible configurar Network Discovery de las siguientes maneras:

Configuración de tareas de detección	En la configuración de Network Discovery, se puede establecer el número máximo de subprocesos por tarea de detección. Durante el proceso de detección, se utiliza otro subproceso para detectar cada dispositivo. Este número es el recuento máximo de subprocesos predeterminado cuando se crea una tarea nueva de Network Discovery. Puede también configurar este recuento para una tarea individual al editar las propiedades avanzadas de la tarea. Puede reducir este valor si la tarea de detección coloca una carga en el rendimiento del servidor.
Clasificaciones de dispositivos SNMP	Cuando se detectan dispositivos SNMP, se puede identificar una clasificación de tipo de dispositivo de red con el recurso. Este método permite identificar recursos, como enrutadores, conmutadores, impresoras, servidores, etc. Es posible configurar las clasificaciones de recursos SNMP detectados. Ver "Clasificación de dispositivos SNMP " en la página 220.

Esta tarea es un paso en el proceso para detectar los dispositivos de red.

Ver "Detección de dispositivos de red" en la página 209.

Para configurar las opciones de detección

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Todas las configuraciones**.
2. En el panel izquierdo, expanda **Configuración > Detección e inventario** y, después, haga clic en **Configuración de Network Discovery**.
3. En la página **Configuración de Network Discovery**, escriba el número máximo de subprocesos por tarea de entrega.

   Durante el proceso de detección, se utiliza otro subproceso para detectar cada dispositivo.

   Este número es el recuento máximo de subprocesos predeterminado cuando se crea una tarea nueva de Network Discovery. Puede también configurar este recuento para una tarea individual al editar las propiedades avanzadas de la tarea.

   Puede reducir este valor si la tarea de detección coloca una carga en el rendimiento del servidor.
4. Haga clic en **Guardar cambios**.

Creación de tareas de Network Discovery con el asistente

El asistente de Network Discovery es una herramienta de administración que lo guía para crear una tarea de detección y configurar las opciones. Es posible editar la configuración avanzada y las programaciones de la tarea más tarde mediante la edición de la tarea.

Esta tarea es un paso en el proceso para detectar los dispositivos de red.

Ver "Detección de dispositivos de red" en la página 209.

Para crear tareas de Network Discovery con el asistente de Network Discovery

1. En Symantec Management Console, en el menú **Inicio**, haga clic en **Detección e Inventario > Network Discovery**.
2. En el elemento web **Acciones de inicio rápido de la Detección de red**, haga clic en **Iniciar el Asistente para detección**.
3. En el asistente, seleccione un método de detección y después haga clic en **Siguiente**.

   Ver "Métodos para detectar dispositivos de red" en la página 216.
4. Especifique las partes de la red que desea detectar y después haga clic en **Siguiente**.

   Ver "Sobre seleccionar los intervalos de red para detectar" en la página 217.
5. Seleccione un perfil de conexión y después haga clic en **Siguiente**.

   Los perfiles de conexión especifican los protocolos que desee utilizar para la detección. Utilice un perfil existente o cree uno nuevo.

   Ver "Cómo crear perfiles de conexión con Network Discovery" en la página 214.

   Ver "Creación o clonación de un perfil de conexión" en la página 215.
6. Establezca el nombre de la tarea y, a continuación, haga clic en **Siguiente**.
7. Programe la tarea y después haga clic en **Finalizar**.

   Ver "Adición de una programación a una política, una tarea o un trabajo" en la página 424.
8. Para ver las tareas que crea el asistente para detección, consulte la parte inferior de la **Página inicial de Network Discovery**

   Quizá necesite hacer clic en el icono de actualización para ver las tareas creadas recientemente.

Creación y modificación manual de tareas de Network Discovery

Es posible crear y modificar manualmente las tareas desde el Portal de administración de tareas. Esta opción permite configurar opciones avanzadas y programaciones. Cuando se crean tareas manualmente, se puede detectar una red o un dispositivo individual.

Esta tarea es un paso en el proceso para detectar los dispositivos de red.

Ver "Detección de dispositivos de red" en la página 209.

Para crear una tarea manualmente para detectar una red

1. En Symantec Management Console, realice una de las siguientes acciones:
   - En el menú **Inicio**, haga clic en **Detección e Inventario > Network Discovery** y, a continuación, en el elemento web **Administración de tareas de Network Discovery**, en la ficha **Tareas disponibles**, haga clic en **Nueva**.
   - En el menú **Administrar**, haga clic en **Tareas y trabajos**. En el panel izquierdo, expanda **Trabajos y tareas de sistema**, haga clic con el botón derecho en **Detección e Inventario** y después haga clic en **Nueva > Tarea**. En el cuadro de diálogo **Crear una nueva tarea**, en el panel izquierdo, en **Detección e Inventario**, haga clic en **Detectar red**.
2. Asigne a la tarea un nombre exclusivo y descriptivo.
3. Seleccione un perfil de conexión.

   Los perfiles de conexión especifican los protocolos que desee utilizar para la detección. Utilice un perfil existente o cree uno nuevo.

   Ver "Cómo crear perfiles de conexión con Network Discovery" en la página 214.

   Ver "Creación o clonación de un perfil de conexión" en la página 215.
4. Seleccione un método de detección.

   Ver "Métodos para detectar dispositivos de red" en la página 216.
5. Especifique las partes de la red que desea detectar.

   Ver "Sobre seleccionar los intervalos de red para detectar" en la página 217.
6. (Opcional) Para configurar el número máximo de dispositivos que desea detectar de forma simultánea, haga clic en **Opciones avanzadas**.
7. Haga clic en **Aceptar**.

8 En la ventana de la tarea que se abre, programe la tarea.

Ver "Adición de una programación a una política, una tarea o un trabajo" en la página 424.

9 Para ver la tarea, en el panel izquierdo, haga clic en **Tareas y trabajos > Trabajos y tareas de sistema > Detección e Inventario**. Quizá necesite hacer clic en el icono de actualización para ver las tareas creadas recientemente.

Para crear una tarea manualmente para detectar un dispositivo individual

1 En Symantec Management Console, en el menú **Administrar**, haga clic en **Tareas y trabajos**. En el panel izquierdo, expanda **Trabajos y tareas de sistema**, haga clic con el botón derecho en **Detección e Inventario** y después haga clic en **Nueva > Tarea**.

2 En el cuadro de diálogo **Crear una nueva tarea**, en el panel izquierdo, en **Detección e Inventario**, haga clic en **Detectar dispositivo**.

3 Asigne a la tarea un nombre exclusivo y descriptivo.

4 Seleccione un perfil de conexión.

Los perfiles de conexión especifican los protocolos que desee utilizar para la detección. Utilice un perfil existente o cree uno nuevo.

Ver "Cómo crear perfiles de conexión con Network Discovery" en la página 214.

Ver "Creación o clonación de un perfil de conexión" en la página 215.

5 Haga clic en **Aceptar** para guardar la tarea.

6 En la ventana de la tarea que se abre, haga clic en **Nueva programación**.

7 En el cuadro de diálogo **Nueva programación**, programe la tarea, especifique el dispositivo que desee detectar escribiendo la dirección IP o el nombre y después haga clic en **Programación**.

Ver "Adición de una programación a una política, una tarea o un trabajo" en la página 424.

8 Para ver la tarea, en el panel izquierdo, haga clic en **Tareas y trabajos > Trabajos y tareas de sistema > Detección e Inventario**. Quizá necesite hacer clic en el icono de actualización para ver las tareas creadas recientemente.

Cómo crear perfiles de conexión con Network Discovery

Las tareas de Detección de red utilizan los perfiles de conexión para configurar los protocolos que se utilizan al comunicarse con los dispositivos de red. Los perfiles de conexión constituyen un componente de la Plataforma de administración

Symantec. La forma en que utilice los protocolos y los perfiles de conexión tiene importantes ramificaciones en la capacidad que Network Discovery tenga para detectar dispositivos.

Network Discovery usa perfiles de conexión para conectarse a los dispositivos de destino mediante los protocolos habilitados en el perfil. Cuando se detecta un dispositivo, se crea un recurso para ese dispositivo en la CMDB. El recurso guarda un registro de los protocolos que se usaron para la comunicación con el dispositivo.

Si se realizan cambios en los perfiles de conexión relacionados con los protocolos usados o las credenciales usadas para esos protocolos, y si se desea detectar los dispositivos que usan esos valores modificados, se deberá ejecutar una detección de nuevo.

Puede crear y utilizar distintos perfiles de conexión según el tipo de dispositivos y protocolos que se empleen en la red. Durante la configuración de las tareas de Detección de red, puede utilizar un perfil de conexión o crear uno.

Ver "Creación de tareas de Network Discovery con el asistente" en la página 212.

Ver "Creación y modificación manual de tareas de Network Discovery" en la página 213.

Para crear un perfil de conexión

1. En una tarea de Detección de red, haga clic en **Nuevo** perfil de conexión.

   Los protocolos de las listas son los que se admiten.
2. Asigne un nombre al perfil de conexión.
3. Active o desactive cada protocolo, defina la configuración operativa y seleccione las credenciales para cada protocolo.

   Ver "Cómo administrar credenciales" en la página 115.
4. Haga clic en **Aceptar**.
5. Seleccione el perfil que desee de la lista desplegable.

Creación o clonación de un perfil de conexión

Los perfiles de conexión almacenan la información necesaria para comunicarse con los equipos y otros dispositivos de red mediante los protocolos de red estándar de supervisión. Estos protocolos incluyen SNMP, WMI, WSMan y otros.

Los perfiles de conexión se asocian a los dispositivos durante la detección de red. Durante la detección, se selecciona un perfil de conexión para definir los protocolos y las credenciales que se deben usar. Cuando la detección finaliza, este perfil de conexión se asocia a cada recurso detectado. Cuando la información se requiere, el perfil de conexión asociado se usa para conectarse.

Generalmente, es necesario crear un nuevo perfil de conexión para cada segmento de la red que use diferentes credenciales de supervisión de red.

Para crear un perfil de conexión

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Todas las configuraciones**.
2. En el panel izquierdo, expanda **Supervisión y alertas >Administración de protocolos > Perfiles de conexión** y, a continuación, haga clic en **Administrar perfiles de conexión**.
3. En la página **Administrar perfiles de conexión**, haga clic en **Agregar configuración** y proporcione un nombre para el nuevo perfil.
4. En el cuadro de diálogo **Definir configuración de grupo**, escriba el nombre del nuevo perfil, habilite los protocolos que desee y proporcione los detalles necesarios del protocolo.

   En la parte superior derecha al lado de cada protocolo que desee habilitar, haga clic en el círculo coloreado y, a continuación, haga clic en **Activado**.

   Para obtener más información, haga clic en la página y después presione **F1**.
5. Haga clic en **Aceptar**.

Métodos para detectar dispositivos de red

Al detectar dispositivos de red, se puede usar uno de los siguientes métodos de detección: ping o ARP.

Ver "Detección de dispositivos de red" en la página 209.

Las tareas de detección se inician con el asistente de Network Discovery, al cual se accede desde la página principal de Network Discovery. Aquí es donde se indica qué método de detección desea usar.

Ver "Creación de tareas de Network Discovery con el asistente" en la página 212.

Ver "Creación y modificación manual de tareas de Network Discovery" en la página 213.

Tabla 13-2 Métodos de detección de red

Método	Descripción
Ping	La existencia de dispositivos se determinada enviando una solicitud ping ICMP a cada dirección IP posible en un intervalo o una subred especificado. Cuando un dispositivo recibe un ping, envía una respuesta para informar de la presencia del dispositivo al motor de detección. Es posible usar este método para realizar una búsqueda completa que encuentre todos los dispositivos. Este método es inútil si su firewall de red no permite solicitudes ping. Este método puede no ser el mejor para subredes pequeñas (con pocos dispositivos en el espacio de dirección). El motor puede pasar mucho tiempo esperar respuestas de dispositivos que no existen. Esta situación ocurre porque el motor espera hasta que el período de tiempo de espera especificado caduque y, a continuación, si corresponde, el motor vuelve a intentarlo una o más veces.
ARP	La existencia de dispositivos es inicialmente determinada leyendo la tabla de memoria caché ARP de un dispositivo de la infraestructura de red (como un conmutador o un enrutador). La tabla de memoria caché ARP se lee en el dispositivo, y se contacta y detecta cada dispositivo de la tabla individualmente. Este método de detección brinda al motor de detección un conjunto de dispositivos para detectar. Sin embargo, las entradas de la tabla de memoria caché ARP se eliminan después de períodos de inactividad relativamente cortos. Esto significa que el análisis por sí mismo no es consciente de dispositivos inactivos. Es posible reparar este problema enviando un ping a cada dispositivo en una red de destino. Este proceso actualiza la tabla, que tiene todos los dispositivos.

Sobre seleccionar los intervalos de red para detectar

Cuando se crea una tarea de Network Discovery, se identifica el único dispositivo de red o los rangos de direcciones que se desea detectar. Para ello, especifique las direcciones que desee incluir o excluir o una combinación de ambas.

Ver "Creación de tareas de Network Discovery con el asistente" en la página 212.

Ver "Creación y modificación manual de tareas de Network Discovery" en la página 213.

Si tiene un dispositivo de origen y después crea un intervalo de inclusión, el dispositivo de origen debe estar incluido dentro del intervalo de inclusión para que también se lo detecte.

Para usar un rango personalizado, se pueden utilizar comodines o rangos de valores en el tercer o cuarto octeto de la dirección. Los siguientes ejemplos muestran cómo se puede usar un rango personalizado:

172.16.[*].[*]	Es posible usar un asterisco como comodín que será equivalente a cualquier valor entre 0 y 254.
172.16.[1-24].[1-254] 172.16.[3-30].[1-10]	Es posible especificar un rango de valores. Cualquier dirección en el intervalo está incluida o excluida.

Es posible también importar un archivo de texto para especificar las direcciones que desee incluir o excluir. Cuando se configura un archivo de texto, es necesario incluir toda la información necesaria para ese tipo de dirección o rango. Por ejemplo, si se especifica un rango de IP, es necesario incluir la dirección IP inicial, la dirección IP final y la máscara. Es posible también especificar rangos de IP personalizados en un archivo de importación.

A continuación, se incluye un ejemplo del formato de un archivo de importación:

```
SingleIpAddr, Include, 192.168.0.2,
SingleIpAddr, Exclude, 192.168.0.3,

Hostname, Include, hostname1.company1.com
Hostname, Exclude, hostname2

Subnet, Include, 192.168.0.0, 255.255.255.0
Subnet, Exclude, 192.169.0.0, 255.255.255.0

CustomIpAddrRange, Include, 192.168.*.*, 255.255.0.0
CustomIpAddrRange, Exclude, 10.192.1-25.1-254, 255.0.0.0
CustomIpAddrRange, Include, 10.192.4.1-100, 255.255.254.0

IpAddrRange, Include, 192.168.0.1, 192.168.0.200, 255.255.255.0
IpAddrRange, Exclude, 192.168.0.120, 192.168.1.140, 255.255.255.0
```

Visualización de dispositivos detectados en vistas organizativas

Cuando se detecta un dispositivo, se crea automáticamente un recurso para dicho dispositivo en la Base de datos de la administración de configuración (CMDB). Puede ver los dispositivos a través de las vistas organizativas. Las vistas organizativas muestran todos los recursos conocidos del entorno. Puede ver todos los dispositivos detectados en una vista denominada Recursos de red. También hay vistas para tipos de recursos individuales, como equipo, impresora de red, etc.

Si se conoce el tipo de recurso del dispositivo, se presenta como propiedad del recurso. Si un dispositivo tiene el tipo 'Recurso de red', quiere decir que se desconoce el tipo de dispositivo. Los dispositivos desconocidos se muestran en la vista Recurso de red y no en las vistas específicas a los tipos de recursos. Si hay dispositivos de clasificación desconocida, puede modificar la lista de clasificaciones de SNMP.

Ver "Clasificación de dispositivos SNMP " en la página 220.

Esta tarea es un paso en el proceso para detectar los dispositivos de red.

Ver "Detección de dispositivos de red" en la página 209.

Para ver los dispositivos detectados en vistas organizativas

1. En Symantec Management Console, en el menú **Administrar**, haga clic en **Todos los recursos**.
2. En el panel izquierdo, expanda **Predeterminado > Todos los recursos > Activo** y, después, haga clic en **Recurso de red**.
3. Para ver un tipo específico de recurso, en el panel izquierdo, haga clic en un tipo de recurso en **Recurso de red**.

Visualización de informes de detección

Puede ver los resultados de la detección a través de informes. Es posible ver los informes predefinidos o crear sus propios informes.

El informe Dispositivos detectados permite filtrar los resultados que se basen en un rango de fechas, en el método o protocolo de detección utilizado, o en la tarea empleada.

El informe Dispositivos detectados por grupo permite agrupar los resultados que se basen en un rango de fechas, en el método o protocolo de detección utilizado, en la tarea empleada o en el tipo de dispositivo.

Esta tarea es un paso en el proceso para detectar los dispositivos de red.

Ver "Detección de dispositivos de red" en la página 209.

Para visualizar informes de detección

1. En Symantec Management Console, en el menú **Informes**, haga clic en **Todos los informes**.
2. En el panel izquierdo, expanda **Informes > Detección e Inventario** y, después, haga clic en el informe que desee ver.
3. Escriba los parámetros del informe y haga clic en **Actualizar**.

   Ver "Acerca de los informes de Notification Server" en la página 439.

Clasificación de dispositivos SNMP

Los dispositivos SNMP detectados se identifican por el tipo de dispositivo, tales como equipo, impresora de red, etc. Para que se detecte el tipo de dispositivo, Network Discovery debe conocer la clasificación de dispositivo SNMP de dicho tipo. Network Discovery contiene una lista predefinida de dispositivos SNMP comunes. Si el dispositivo que se está detectando está en la lista, entonces se podrá identificar. Si el dispositivo no está en la lista, se lo identifica con el tipo de recurso genérico **Recurso de red**.

Puede ver la lista predefinida en la página **Clasificaciones de dispositivos**. Esta página contiene una lista de las clasificaciones de los dispositivos utilizados comúnmente. Dichos datos incluyen el Id. de objeto SNMP, el tipo de dispositivo, el fabricante y el modelo del dispositivo. Si el Id. de objeto SNMP que se detecta coincide con un elemento de la lista, se rellenan los datos.

Antes de ejecutar una tarea de detección de redes, puede consultar la lista de clasificaciones de dispositivos, la cual contiene fabricantes comunes. Si descubre que la lista está incompleta, puede agregar o editar las clasificaciones para adaptar la lista al entorno de red. Si se toma el tiempo de analizar y personalizar la lista de clasificaciones de dispositivos obtendrá datos de detección más completos. No se requiere realizar esta tarea antes de la detección. Puede realizar la tarea después de una detección, sin embargo, tendrá que volver a ejecutar la detección para obtener la clasificación actualizada.

Si cambia la información para una clasificación existente del dispositivo SNMP, deberá volver a analizar cualquier dispositivo que haya sido clasificado previamente usando esa entrada. Es necesario volver a analizar para reclasificar los dispositivos con la información cambiada.

Tras ejecutar una tarea de detección de redes, es probable que haya dispositivos con una clasificación desconocida. Si conoce el Id. de objeto de dichos objetos, podrá agregarlos a la lista de clasificaciones. La próxima vez que ejecute una tarea de detección de redes, los dispositivos utilizarán la lista actualizada para su clasificación.

Puede configurar los valores de clasificación de dispositivos SNMP que se utilizan para identificar los dispositivos SNMP. Se proporciona una lista de dispositivos comunes en Network Discovery. Puede agregar, editar o eliminar las clasificaciones a fin de adaptar la lista al entorno de red. Una vez que cambia una clasificación de dispositivo, se debe volver a detectar para poderse reclasificar.

Esta tarea es un paso en el proceso para detectar los dispositivos de red.

Ver "Detección de dispositivos de red" en la página 209.

Para clasificar dispositivos SNMP

1. En Symantec Management Console, en el menú **Inicio**, haga clic en **Detección e Inventario > Network Discovery**.
2. En el elemento web **Acciones de inicio rápido de la Detección de red**, haga clic en **Clasificaciones de dispositivos SNMP**.
3. Para agregar una clasificación nueva, haga clic en **Agregar** y escriba la información acerca del dispositivo.

   El Id. de objeto SNMP debe ser un valor único que puede obtener a través del fabricante del dispositivo.
4. También puede editar o quitar las clasificaciones para que coincidan con los dispositivos del entorno de red.
5. Para volver a clasificar los dispositivos que se basan en la configuración nueva, debe volver a ejecutar la detección.

Delegar tareas de Network Discovery a usuarios que no son administradores

Como administrador de red, puede tener un equipo de administradores a quienes delegar ciertas tareas de administración de la red. Independientemente de si trabaja solo o con un equipo de administradores, es posible que necesite delegar las tareas de detección de redes a usuarios que no sean administradores.

Las tareas de detección de redes necesitan derechos para trabajar con perfiles de conexión y credenciales. Estos derechos se conceden mediante una combinación de permisos y de privilegios. Los permisos se asignan de forma predeterminada a elementos, como archivos, tareas y asistentes. Los privilegios se conceden a los roles de usuario, incluido el rol de administrador predefinido y los roles predefinidos de usuarios que no son administradores. La intersección de los permisos del elemento y de los privilegios del rol determina qué pueden hacer a los elementos los administradores y los usuarios que no lo son.

Ver "Acerca de Network Discovery" en la página 208.

Cada uno de los roles predefinidos de usuarios que no son administradores en Symantec Management Platform incluye privilegios inherentes.

Ver "Roles de seguridad predefinidos" en la página 107.

Ver "Categorías de privilegios de seguridad" en la página 489.

Para permitir a usuarios detectar los dispositivos de red y trabajar con perfiles de conexión y credenciales, asigne privilegios a los roles de usuario que permitan a esos roles crear perfiles de conexión y credenciales. A continuación, se selecciona un rol de usuario que no es administrador al cual se asignan usuarios. Después, limita o aumenta el ámbito del rol quitando o asignando privilegios específicos. Para crear y ejecutar tareas de detección de redes, el rol de usuario debe tener acceso por lo menos a un perfil de conexión predeterminado. Este perfil puede ser el perfil de conexión predeterminado.

El rol de Supervisores de Symantec es un rol de alto nivel de usuarios que no son administradores. Se puede asignar un rol con derechos inherentes limitados a otros empleados. Los roles de Empleados de Symantec Nivel 1 y de Empleados de Symantec Nivel 2 son buenos ejemplos. Estos roles se usan en algunas de las tareas que se incluyen en el proceso que se define en este tema. Usted no está limitado a estos roles. Son los roles predefinidos más útiles para los administradores.

Es posible delegar tareas a más de un rol de usuario. Para crear, editar o ejecutar tareas, un usuario debe ser miembro de un rol de seguridad que tenga el privilegio Administración de tareas de Discovery.

El rol de Supervisores de Symantec predeterminado incluye más acceso a la detección de redes que otros roles de usuarios que no son administradores. Delegar tareas al rol de Supervisores de Symantec es menos complicado que delegar tareas a los roles que no tienen ningún acceso a la realización de tareas de detección de redes.

Seleccione un rol al cual delegar tareas según lo que desee que los usuarios que no son administradores puedan hacer. Para delegar tareas, realice cada paso del proceso en orden. Las tareas que se detallan en pasos posteriores pueden depender de los derechos que se concedan en pasos precedentes.

Tabla 13-3 Proceso para delegar tareas de Network Discovery a usuarios que no son administradores

Paso	Tarea	Descripción
Paso 1	Agregar usuarios que no sean administradores a roles de seguridad para realizar tareas de detección de redes.	Para delegar tareas a los usuarios en roles que no son de administrador, es necesario asignar usuarios a esos roles. Ver "Agregar usuarios que no sean administradores a roles de seguridad para realizar tareas de Network Discovery" en la página 224.

Paso	Tarea	Descripción
Paso 2	Habilitar los roles que no son de administrador para crear o para ejecutar tareas de detección de redes	Es posible delegar tareas de detección de redes a los roles que no son de administrador y asignar usuarios que no sean administradores a esos roles. Varios roles predeterminados se incluyen en Symantec Management Platform y cada uno tiene ciertos derechos inherentes. El rol de Supervisores de Symantec puede ejecutar tareas de detección de redes. Los demás roles que no son de administrador pueden incluso ejecutar tareas existentes hasta que se concedan los privilegios necesarios al rol. Es necesario realizar ciertos pasos para permitir al rol que no es de administrador crear y ejecutar tareas de detección de redes. De forma predeterminada, los administradores, los Supervisores de Symantec y los empleados de Symantec Nivel 1 y Nivel 2 pueden ver la página del portal de la detección de redes. Esta página es una ubicación conveniente desde la cual los administradores ven y ejecutan las tareas de detección de redes. Los administradores y los supervisores pueden ver todas las piezas de esta página de forma predeterminada. Sin embargo, el elemento web de la administración de tareas de detección de redes se deshabilita para los usuarios. Para permitir que otros usuarios que no son administradores vean y usen este elemento web, asígnelos a un rol de seguridad que tenga el privilegio Administración de tareas de Discovery habilitado. Ver "Roles de seguridad predefinidos" en la página 107. Ver "Cómo habilitar los roles que no son de administrador para crear o ejecutar tareas de Network Discovery" en la página 226.
Paso 3	(Opcional pero recomendado) Conceda privilegios para crear credenciales y perfiles de conexión a los roles que no sean de administrador.	Se pueden otorgar privilegios para detectar los dispositivos de red y para crear o para editar credenciales y perfiles de conexión a un rol que no es de administrador. Crear o editar credenciales y perfiles de conexión puede ser necesario para realizar las tareas que se detallan más adelante en este proceso. Este paso es opcional porque los usuarios pueden crear tareas de detección de redes sin estos privilegios. Tendrían que simplemente usar los perfiles de conexión existentes a los cuales tienen acceso. Ver "Categorías de privilegios de seguridad" en la página 489. Ver "Cómo conceder privilegios para crear credenciales y perfiles de conexión a los roles que no sean el de administrador" en la página 229.
Paso 4	Conceda acceso de roles que no sean de administrador al perfil de conexión predeterminado.	Para crear y ejecutar tareas de detección de redes, un rol de usuario debe tener acceso al perfil de conexión predeterminado (o a otro perfil de conexión, pero por lo menos uno). Ver "Concesión de acceso a roles que no sean de administrador al perfil de conexión predeterminado" en la página 230.

Paso	Tarea	Descripción
Paso 5	Habilite roles que no sean los roles de seguridad predefinidos para crear y ejecutar tareas usando el Asistente de Detección de red	Los roles de seguridad siguientes están predefinidos y, de forma predeterminada, pueden crear y ejecutar tareas usando el Asistente de Detección de red: ■ Administrador ■ Supervisores de Symantec ■ Trabajadores del nivel 2 de Symantec ■ Trabajadores del nivel 1 de Symantec Si es necesario permitir que otros roles creen y ejecuten tareas usando el asistente, debe darles acceso explícitamente. Ver "Habilitación de roles que no sean los roles de seguridad predefinidos para crear y ejecutar tareas usando el asistente de Network Discovery" en la página 231.
Paso 6	(Opcional) Haga que un perfil de conexión sea de solo lectura.	Si desea permitir a un rol específico que no sea el de administrador ver, pero no editar un perfil de conexión, puede hacer el perfil de solo lectura. Ver "Cómo realizar un perfil de conexión de solo lectura" en la página 232.

Agregar usuarios que no sean administradores a roles de seguridad para realizar tareas de Network Discovery

Si desea delegar tareas de Network Discovery a los usuarios que no son administradores, estos deben tener los privilegios necesarios para realizar esas tareas. Los privilegios son asignados a los roles de usuario. Si no ha creado un usuario Windows para realizar tareas de Network Discovery, deberá crear este usuario primero. A continuación, agregue el usuario a su rol de seguridad elegido o cree un rol personalizado. Finalmente, otorgue privilegios al rol de seguridad. Es posible entonces delegar las tareas para las que el rol tiene suficientes privilegios.

La página del portal de Network Discovery es una ubicación conveniente donde puede ver y realizar tareas de detección. Los administradores y supervisores de Symantec tienen total acceso a esta página de forma predeterminada. Los usuarios en otros role que no son de administrador pueden ver esta página. Sin embargo, el componente Web part **Administración de tareas de Discovery** está deshabilitado a menos que se lo habilite con el privilegio de Administración de tareas de Discovery. Al agregar usuarios que no son administradores a los roles de seguridad y conceder los derechos para la administración de tareas de Network Discovery, les permite ver esta página y trabajar en ella.

Ver "Cómo habilitar los roles que no son de administrador para crear o ejecutar tareas de Network Discovery" en la página 226.

Symantec Management Platform incluye varios roles no administradores de seguridad predefinidos de forma predeterminada. Es posible también crear roles de seguridad personalizados.

Ver "Roles de seguridad predefinidos" en la página 107.

Ver "Creación y configuración de las cuentas de usuario Symantec Management Platform" en la página 225.

Esta tarea es un paso en el proceso de delegación de tareas de Network Discovery a los usuarios que no son administradores.

Ver "Delegar tareas de Network Discovery a usuarios que no son administradores" en la página 221.

Para agregar usuarios que no sean administradores a roles de seguridad para realizar tareas de Network Discovery

1. Inicie sesión en Symantec Management Console como administrador.
2. Para crear un nuevo usuario de Windows, haga lo siguiente:
   - En Symantec Management Console, en el menú **Configuración**, haga clic en **Seguridad > Administración de cuentas**.
   - En el panel izquierdo, haga clic en **Cuentas**.
   - En la página **Cuentas**, haga clic en **Agregar**.
   - En el cuadro de diálogo **Cuenta nueva**, escriba un nombre para el nuevo usuario y haga clic en **Aceptar**.
   - En el panel derecho, en la ficha **General**, en **Detalles de cuenta**, en el campo **Nombre completo**, escriba el nombre completo del usuario.
     Es posible dejar el campo **Correo electrónico** vacío. No es necesario para este procedimiento.
   - En **Credenciales**, haga clic en **Agregar credencial > Windows**.
   - En el cuadro de diálogo **Credencial de Windows**, escriba el nombre de inicio de sesión que se corresponde con el usuario de Windows asociado a esta nueva cuenta y haga clic en **Aceptar**.
   - Habilite la cuenta.
     En la parte superior derecha de la página, haga clic en el círculo coloreado y, después, en **Activado**.
3. Para agregar el usuario a un rol de seguridad al cual desee delegar tareas, haga lo siguiente:
   - En la ficha **Miembro de**, haga clic en **Agregar rol**.

- En el cuadro de diálogo **Seleccionar roles**, haga clic en el **Empleados de Symantec Nivel 1** u otro rol al cual desee asignar este usuario y después haga clic en **Aceptar**.
  Si ninguno de los roles de seguridad predefinidos cubre sus necesidades, puede crear un rol de seguridad personalizado.
  Ver "Creación y configuración de roles de seguridad" en la página 89.

4 Haga clic en **Guardar cambios**.

Cómo habilitar los roles que no son de administrador para crear o ejecutar tareas de Network Discovery

Es posible delegar tareas de detección de redes a los usuarios fuera del grupo de administradores de Symantec. Para delegar tareas, se asignan privilegios a los roles que no son de administrador. A continuación, agregue usuarios a esos roles que no son de administrador.

Este tema describe cómo delegar tareas de Network Discovery comunes a los siguientes roles que no son de administrador:

- Supervisores de Symantec.
  De forma predeterminada, los usuarios en este rol pueden ejecutar tareas de detección de redes existentes. Sin embargo, no pueden crear tareas de forma predeterminada. Esto se debe a que no tienen acceso al perfil de conexión predeterminado, a menos que les conceda acceso explícitamente.
- Empleados de Symantec Nivel 1 y Nivel 2.
  Los usuarios en estos roles tienen derechos limitados. Ni siquiera pueden ejecutar tareas existentes hasta que usted les dé derecho para hacerlo.

Usted no está limitado a usar estos roles que no son de administrador. Se muestran en este tema como ejemplos. Use el rol de seguridad predefinido que necesite.

Ver "Roles de seguridad predefinidos" en la página 107.

Las tareas usan perfiles de conexión, que usan credenciales. Para que cualquier rol que no es de administrador cree tareas (y no las ejecute simplemente), es necesario configurar permisos de acceso para un perfil de conexión. A continuación, configure un nivel de control (el nivel máximo es **Control completo**) a la configuración del protocolo de ese rol. Una vez que haya configurado estos permisos, los usuarios cuyo rol no sea administrador pueden realizar las tareas que usted especifica.

Para permitir que los usuarios que no son administradores creen tareas de Network Discovery, es necesario completar los procedimientos siguientes:

- Otorgue derechos a un rol que no sea de administrador para la administración de tareas de Network Discovery. Este procedimiento permite a los usuarios en el rol ejecutar tareas.
- Agregue el rol que desee a los permisos de acceso del perfil de conexión relevante. A continuación, permita que este rol controle la configuración del protocolo. Una vez que se agrega el rol a un perfil de conexión, los usuarios en ese rol pueden crear y editar tareas de Network Discovery.

Esta tarea es un paso en el proceso de delegación de tareas de Network Discovery a los usuarios que no son administradores.

Ver "Delegar tareas de Network Discovery a usuarios que no son administradores" en la página 221.

Para otorgar derechos a un rol que no sea de administrador para la administración de tareas de Network Discovery

1. Inicie sesión en Symantec Management Platform como administrador.
2. En Symantec Management Console, en el menú **Configuración**, haga clic en **Seguridad > Administración de cuentas**.
3. En el panel izquierdo, en **Administración de cuentas**, haga clic en **Roles**.
4. En la página **Roles**, en el panel izquierdo, haga clic en el rol que no es de administrador al cual desea delegar la creación y ejecución de tareas de Network Discovery.

   Los roles típicos a los cuales los administradores delegan estas tareas son Empleados de Symantec Nivel 1 y Empleados de Symantec Nivel 2.
5. En la derecha, en la ventana que se etiqueta con el rol que usted seleccionó, haga clic en la ficha **Privilegios** si no está activa.
6. En **Privilegios de administración**, seleccione **Administración de tareas de Discovery**.
7. Si el rol que se ha seleccionado además necesita crear o editar perfiles de conexión, seleccione las siguientes opciones adicionales:
   - En **Privilegios de perfil de conexión**, seleccione **Crear perfil de conexión**.
   - En **Privilegios del sistema**, seleccione **Ver seguridad**.
   - En **Privilegios de credenciales**, seleccione **Crear credencial**.
8. Haga clic en la ficha **Miembros**.

9 Asegúrese de que el usuario que desee agregar al rol seleccionado se haya agregado a este rol.

Si el usuario no es miembro de este rol, deberá crear un usuario de Notification Server y agregar el usuario al rol relevante.

Ver "Agregar usuarios que no sean administradores a roles de seguridad para realizar tareas de Network Discovery" en la página 224.

10 Haga clic en **Guardar cambios**.

Para conceder un rol predefinido completo (o menor) a la configuración del protocolo

1 En Symantec Management Console, en el menú **Configuración**, haga clic en **Todas las configuraciones**.

2 En el panel izquierdo, en **Configuración**, expanda **Supervisión y alertas > Administración de protocolos > Perfiles de conexión** y haga clic en **Administrar perfiles de conexión**.

3 En la página **Administrar perfiles de conexión**, haga clic en **Perfil de conexión predeterminado** y después haga clic en **Editar**.

4 En el cuadro de diálogo **Definir configuración de grupo**, haga clic en **Permisos de acceso a la configuración de protocolos**.

5 Haga clic en **Agregar**, seleccione el rol al cual desee otorgar control y haga clic en **Seleccionar**.

Empleados de Symantec Nivel 1	De forma predeterminada, los usuarios en este rol tienen menos derechos que los Supervisores de Symantec. Cuando se otorga el control completo y privilegios de administración de tareas de detección, estos empleados pueden crear y ejecutar tareas de detección de redes.
Empleados de Symantec Nivel 2	Los usuarios en este rol tienen menos derechos de forma predeterminada. Cuando se otorga el control completo y privilegios de administración de tareas de detección, estos empleados pueden crear y ejecutar tareas de detección de redes.
Supervisores de Symantec	Los usuarios en este rol pueden ejecutar tareas de detección de redes de forma predeterminada. Cuando se otorga el control completo, estos empleados pueden además crear y editar tareas de detección de redes.

6 En el cuadro de diálogo **Selección de permisos**, seleccione permisos en una de las siguientes formas:

- Seleccione **Uso** y **Leer**. Es posible seleccionar cualquier otro cuadro que corresponda a las tareas que desee que el rol seleccionado pueda realizar. A continuación, haga clic en **Seleccionar**.
- Haga clic en **Control completo** para dar al rol todos los derechos disponibles detallados y después haga clic en **Seleccionar**.

7 En el cuadro de diálogo **Configuración de descriptor de seguridad para perfil de conexión predeterminado**, haga clic en **Aplicar**.

8 En el cuadro de diálogo **Definir configuración de grupo**, haga clic en **Aceptar** para guardar el perfil de conexión.

Cómo conceder privilegios para crear credenciales y perfiles de conexión a los roles que no sean el de administrador

Cuando se delegan tareas a roles que no son de administrador, es necesario determinar qué tareas pueden realizar los usuarios a los cuales se les asignan esos roles. Cada rol de seguridad predefinido de Symantec Management Platform incluye derechos inherentes.

Ver "Roles de seguridad predefinidos" en la página 107.

Un ejemplo es el rol predeterminado de Supervisores de Symantec. Los usuarios que son asignados a este rol pueden ejecutar tareas existentes sin que se concedan privilegios adicionales al rol. Estos usuarios pueden además crear tareas de detección de redes si tienen acceso a un perfil de conexión existente.

Sin embargo, para permitir que roles que no sean de administrador creen tareas y perfiles de conexión, conceda privilegios a esos roles para crear credenciales y perfiles de conexión. Estos privilegios adicionales son necesarios si se espera que los usuarios creen tareas que pueden necesitar credenciales y perfiles de conexión diferentes de las credenciales y de los perfiles existentes.

Ver "Cómo establecer la configuración de detección" en la página 210.

Para permitir a los usuarios a los que se les asignan roles que no son de administrador crear credenciales y perfiles de conexión, es necesario habilitar esos privilegios para el rol. Estos privilegios permiten a los usuarios crear las credenciales y los perfiles de conexión que se adaptan a las tareas que usted les delega o que ellos crean.

Esta tarea es un paso en el proceso de delegación de tareas de detección de redes a los usuarios que no son administradores.

Ver "Delegar tareas de Network Discovery a usuarios que no son administradores" en la página 221.

Para otorgar privilegios de roles que no sean el de administrador para crear credenciales y perfiles de conexión

1. Inicie sesión en Symantec Management Console como administrador.
2. En Symantec Management Console, en el menú **Configuración**, haga clic en **Seguridad > Administración de cuentas**.
3. En **Administración de cuentas**, haga clic en **Roles**
4. En la página **Roles**, haga clic en el rol que desea habilitar y, en el panel derecho, haga clic en la ficha **Privilegios**.
5. Desplácese a **Privilegios de perfil de conexión** y seleccione **Crear perfil de conexión**.
6. Desplácese a **Privilegios de credencial** y seleccione **Crear credencial**.
7. Desplácese a **Privilegios del sistema** y seleccione **Ver seguridad**.
8. Haga clic en **Guardar cambios**.

Concesión de acceso a roles que no sean de administrador al perfil de conexión predeterminado

Los usuarios en los roles que no son de administrador, necesitan acceder al perfil de conexión predeterminado para ejecutar tareas. Una vez que se concede a estos roles acceso al perfil de conexión predeterminado, los usuarios en esos roles pueden además crear tareas. No pueden crear perfiles de conexión, sino que pueden crear tareas que usan perfiles de conexión existentes.

Esta tarea es un paso en el proceso de delegación de tareas de detección de redes a los usuarios que no son administradores.

Ver "Delegar tareas de Network Discovery a usuarios que no son administradores" en la página 221.

Para conceder a un rol predefinido control completo (o menos) al perfil de conexión predeterminado

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Todas las configuraciones**.
2. En el panel izquierdo, en **Configuración**, expanda **Supervisión y alertas > Administración de protocolos > Perfiles de conexión** y haga clic en **Administrar perfiles de conexión**.
3. En la página **Administrar perfiles de conexión**, haga clic en **Perfil de conexión predeterminado** y después haga clic en **Editar**.
4. En el cuadro de diálogo **Definir configuración de grupo**, haga clic en **Permisos de acceso a la configuración de protocolos**.

Habilitación de roles que no sean los roles de seguridad predefinidos para crear y ejecutar tareas usando el asistente de Network Discovery

El asistente de detección de redes es una herramienta de administrador agrupada con Symantec Management Platform. Es un método para detectar dispositivos de red y realizar otras tareas de detección.

Se accede al asistente de detección de redes desde el menú **Inicio** de Symantec Management Console.

Ver "Creación de tareas de Network Discovery con el asistente" en la página 212.

Los roles de seguridad siguientes están predefinidos y, de forma predeterminada, pueden crear y ejecutar tareas usando el Asistente de Detección de red:

- Administrador
- Supervisores de Symantec
- Trabajadores del nivel 2 de Symantec
- Trabajadores del nivel 1 de Symantec

Se recomienda permitir a otros roles crear y ejecutar tareas desde el Asistente de Detección de red. En este caso, debe otorgar a esos roles los privilegios necesarios para realizar esas tareas usando el asistente.

Esta tarea es un paso en el proceso de delegación de tareas de detección de redes a los usuarios que no son administradores.

Ver "Delegar tareas de Network Discovery a usuarios que no son administradores" en la página 221.

Para permitir roles que no sean roles de seguridad predefinidos para crear tareas usando el Asistente de Detección de red

1. Inicie sesión en Symantec Management Platform como administrador.
2. En Symantec Management Console, en el menú **Configuración**, haga clic en **Seguridad > Permisos**.
3. En **Administrador de roles de seguridad**, en el cuadro desplegable **Rol**, seleccione el rol que desee habilitar.
4. En la lista desplegable **Ver**, haga clic en **Configuración**.
5. En el panel izquierdo, haga clic en **Editar**.

   Tenga en cuenta que en el cuadro de diálogo **Selector de elementos**, si se selecciona la casilla de verificación **Configuración**, todas las opciones se muestran en color gris.

6 Si **Configuración**, está seleccionado, anule la selección.

7 En **Detección e Inventario**, seleccione **Asistente de Detección de red** si no está seleccionado.

8 Vuelva a seleccionar **Configuración** para activar la herencia nuevamente.

9 Haga clic en **Guardar cambios**.

Para habilitar roles que no sean los roles de seguridad predefinidos para crear y ejecutar tareas usando el Asistente de Detección de red

1 Inicie sesión en Symantec Management Platform como administrador.

2 En Symantec Management Console, en el menú **Configuración**, haga clic en **Seguridad > Permisos**.

3 En **Administrador de roles de seguridad**, en el cuadro desplegable **Rol**, haga clic en el rol que desee habilitar.

4 En el cuadro desplegable **Ver**, haga clic en **Tareas**.

5 En el panel izquierdo, en **Tareas**, expanda **Tareas y trabajos > Trabajos y tareas de sistema** y haga clic en **Detección e Inventario**.

Tenga en cuenta que en el panel **Detección e Inventario**, la sección **Heredado** aparece en gris y no se puede editar.

6 En el panel **Detección e Inventario**, en **No heredado**, desplácese hasta **Permisos de Task Server** y seleccione **Ejecutar tarea**.

7 Haga clic en **Guardar cambios** y cierre el **Administrador de roles de seguridad**.

Cómo realizar un perfil de conexión de solo lectura

Es posible que sea necesario delegar las tareas de detección de redes a los usuarios que no tengan rol de administrador. Sin embargo, es posible que no desee que estos usuarios cambien los perfiles de conexión. Se efectuaría un perfil de conexión de sólo lectura para evitar el hacking y para mantener la seguridad y la privacidad de la información confidencial. Otro motivo para efectuar un perfil de conexión de sólo lectura es evitar que los usuarios menos experimentados modifiquen un perfil de conexión para usar protocolos no admitidos.

Si desea limitar la vista de credenciales y la ejecución de tareas de detección de redes de los usuarios, puede bloquear los derechos de escritura de cada perfil de conexión. Mediante el bloqueo de derechos de escritura de usuarios sin rol de administrador, realiza un perfil de conexión de solo lectura para usuarios con ese rol. Los usuarios que son asignados a los roles que no son de administrador cuyos derechos de escritura desea bloquear aún pueden ver y ejecutar tareas, pero no pueden cambiar ese perfil de conexión ni crear un perfil de conexión.

Esta tarea es un paso en el proceso de delegación de tareas de detección de redes a los usuarios que no son administradores.

Ver "Delegar tareas de Network Discovery a usuarios que no son administradores" en la página 221.

Para realizar un perfil de conexión de solo lectura

1. Inicie sesión en Symantec Management Console como administrador.
2. En Symantec Management Console, en el menú **Configuración**, haga clic en **Todas las configuraciones**.
3. En el panel izquierdo, en **Configuración**, expanda **Supervisión y alertas > Administración de protocolos > Perfiles de conexión** y haga clic en **Administrar perfiles de conexión**.
4. En el panel **Administrar perfiles de conexión**, haga clic en **Perfil de conexión predeterminado** y después haga clic en **Editar**.
5. En el cuadro de diálogo **Definir configuración de grupo**, haga clic en **Permisos de acceso a la configuración del protocolo**.
6. En el cuadro de diálogo **Configuración de descriptor de seguridad para perfil de conexión predeterminado**, seleccione el rol, como **Empleados de Symantec Nivel 2** y haga clic en **Editar**.
7. En el cuadro de diálogo **Selección de permisos**, anule la selección en **Escribir** y haga clic en **Seleccionar**.
8. En el cuadro de diálogo **Configuración de descriptor de seguridad para perfil de conexión predeterminado**, haga clic en **Aplicar** para guardar la configuración, en el cuadro de diálogo **Definir configuración de grupo** y en **Aceptar** para guardar el perfil de conexión.

Importación de archivos MIB

Es posible usar dos métodos para importar archivos MIB en la base de datos. Es posible importar manualmente archivos MIB uno a la vez usando la utilidad Importación MIB. Es posible también crear y programar una tarea que importe uno o más archivos MIB.

Para importar archivos MIB manualmente usando la utilidad Importación MIB

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Todas las configuraciones**.
2. En el panel izquierdo, expanda **Supervisión y alertas > Navegador MIB SNMP** y después haga clic en **Navegador MIB**.

3 En la página **Navegador MIB**, haga clic en **Importar el archivo MIB**.

4 En el cuadro de diálogo **Importar el archivo MIB**, haga clic en **Buscar**, seleccione el archivo y después haga clic en **Importar**.

Es posible importar cualquier archivo MIB adicional que se necesite.

Para importar archivos MIB usando la tarea Importar MIB

1 En Symantec Management Console, en el menú **Administrar**, haga clic en **Tareas y trabajos**.

2 En el panel izquierdo, haga clic con el botón derecho en la carpeta donde desee guardar la tarea y haga clic en **Nueva > Tarea**.

3 En el cuadro de diálogo **Crear una nueva tarea**, en el panel izquierdo, en **Supervisión y alertas**, haga clic en **Importar MIB**.

4 Cambie el nombre de la tarea, seleccione el archivo MIB para cargar y especifique la opción de importación.

Es posible elegir importar el único archivo MIB o se puede elegir importar los archivos adicionales MIB que se almacenan en la ubicación de directorio.

5 Haga clic en **Cargar** para cargar el archivo MIB en la tarea de la importación.

6 Si desea importar varios archivos MIB, continúe navegando y cargue cada archivo MIB que necesite en la tarea.

7 Haga clic en **Aceptar**.

8 Seleccione la nueva tarea de importación MIB.

De forma predeterminada, la nueva tarea de importación de MIB se almacena en: **Trabajos y tareas de sistema > Notification Server**.

9 Programe la nueva tarea de importación de MIB para que se ejecute usando la utilidad de programación de tareas.

Ver "Adición de una programación a una política, una tarea o un trabajo" en la página 424.

Sección 4

Cómo instalar y configurar Symantec Management Agent

- Capítulo 14. Introducción a Symantec Management Agent
- Capítulo 15. Instalar Symantec Management Agent en los equipos cliente
- Capítulo 16. Actualizar y desinstalar Symantec Management Agent
- Capítulo 17. Cómo configurar Symantec Management Agent

Capítulo 14

Introducción a Symantec Management Agent

En este capítulo se incluyen los temas siguientes:

- Acerca de Symantec Management Agent
- Acerca del registro de agente

Acerca de Symantec Management Agent

Symantec Management Agent es el software que establece la comunicación entre el equipo con Notification Server y los equipos de la red. Los equipos con Symantec Management Agent instalado se llaman equipos administrados. Los equipos con Notification Server interactúan con Symantec Management Agent para supervisar y administrar cada equipo desde Symantec Management Console.

El equipo con Notification Server y Symantec Management Agent funcionan juntos para proporcionar los siguientes tipos de funcionalidades a los equipos administrados:

- Supervisar hardware y software
- Programar instalaciones de software y actualizaciones de archivo
- Recopilar la información básica del inventario
- Administrar políticas y paquetes

Es posible instalar Symantec Management Agent en equipos con Windows, Linux, UNIX y Mac. Symantec Management Agent además permite instalar y administrar los complementos del agente de solución que proporcionan funcionalidades adicionales al agente. Por ejemplo, la instalación del complemento de Inventory permite recopilar información detallada de hardware y software de todos los equipos administrados.

Ver "Métodos para instalar Symantec Management Agent" en la página 238.

Si desea usar la administración habilitada para la nube, hay un procedimiento especial para instalar y configurar Symantec Management Agent para que funcione en este entorno.

Ver "Acerca de la administración habilitada para la nube" en la página 284.

Acerca del registro de agente

Junto con la función de administración habilitada para la nube que le permite administrar los dispositivos que están fuera del firewall, la función de registro de agente se agregó en IT Management Suite 7.5 para asegurarse de que solamente los equipos cliente de confianza se puedan comunicar con Notification Server.

Ver "Acerca de la administración habilitada para la nube" en la página 284.

La función de registro de agente requiere un equipo cliente para poder comunicarse con Notification Server antes de que pueda ser administrada por este Notification Server. La política predeterminada de registro de agente permite que todos los equipos se comuniquen con Notification Server. Sin embargo, puede crear políticas personalizadas de registro de agente para permitir o bloquear ciertos equipos.

Ver "Crear una política de registro de agente" en la página 243.

Una vez que la política de registro de agente permite o bloquea un equipo, puede cambiar solamente el estado manualmente en la página del informe **Estado de registro del agente**. Por ejemplo, puede permitir o bloquear los equipos que están en estado pendiente. Es posible también revocar el registro de los agentes que tiene previamente permitidos.

Ver "Ver y administrar el estado de registro del agente" en la página 251.

El registro de agente se admite en las plataformas Windows, UNIX, Linux y Mac.

Capítulo 15

Instalar Symantec Management Agent en los equipos cliente

En este capítulo se incluyen los temas siguientes:

- Métodos para instalar Symantec Management Agent
- Instalar Symantec Management Agent en equipos con Windows
- Instalar Symantec Management Agent manualmente en equipos con UNIX, Linux y Mac

Métodos para instalar Symantec Management Agent

Antes de instalar Symantec Management Agent, recomendamos que planifique su instalación usando la *Guía de implementación y planificación de IT Management Suite*.

Es posible instalar Symantec Management Agent en equipos con Windows, UNIX, Linux y Mac.

Ver "Acerca de Symantec Management Agent" en la página 236.

Una vez instalado Symantec Management Agent en el equipo cliente, el agente envía una solicitud de registro a Notification Server para establecer una comunicación de confianza.

Ver "Acerca del registro de agente" en la página 237.

Si desea usar la administración habilitada para la nube, hay un procedimiento especial para instalar y configurar Symantec Management Agent para que funcione en este entorno.

Ver "Acerca de la administración habilitada para la nube" en la página 284.

Tabla 15-1 Métodos para instalar Symantec Management Agent

Método	Descripción
Instalación manual en modo push	La instalación push se inicia en Symantec Management Console e instala Symantec Management Agent de inmediato. Es posible instalar Symantec Management Agent en cualquier cantidad de equipos en la misma operación de instalación push. También puede actualizar las opciones de instalación para cada operación de instalación automática. Para equipos con UNIX, Linux y Mac, este método requiere que se esté ejecutando un servidor de SSH. Además, se debe configurar el firewall para aceptar conexiones SSH en los equipos de destino. Ver "Cómo instalar Symantec Management Agent para Windows manualmente en modo push" en la página 246. Ver "Cómo instalar Symantec Management Agent para UNIX, Linux y Mac manualmente en modo push" en la página 260. Los agentes que instala con la instalación manual en modo push omiten el proceso de registro del agente, y la comunicación entre el agente y Notification Server se establece de forma automática.
Instalación manual en modo pull	La instalación remota se inicia en el equipo donde se instalará Symantec Management Agent. Esta operación permite esquivar las limitaciones de firewall y de acceso de red que pudieran prevenir las instalaciones manuales en equipos remotos. Para equipos UNIX, Linux y Mac, es necesario usar este método si SSH no está disponible. Ver "Cómo instalar Symantec Management Agent para Windows con instalación manual en modo pull" en la página 247. Ver "Cómo instalar Symantec Management Agent para UNIX, Linux y Mac manualmente en modo pull" en la página 264.

Método	Descripción
Instalación automática programada	Este método está disponible para equipos Windows solamente. La instalación programada de Symantec Management Agent se realiza a una hora definida, a diferencia de las instalaciones push manuales que se realizan de forma inmediata. Puede realizar la instalación push de Symantec Management Agent en los equipos de un grupo organizativo, filtro o recurso de destino, o en equipos que tengan recursos seleccionados. Tenga en cuenta que los agentes que instala mediante una instalación automática programada no omiten el proceso de registro de agentes. Ver "Realizar una instalación programada de Symantec Management Agent para Windows" en la página 249.
Directiva de actualización de agente	La política de actualización de Symantec Management Agent se proporciona con Symantec Management Platform. Puede activar dicha política y configurarla a fin de garantizar que todos los equipos administrados tengan instalada la versión correcta de Symantec Management Agent. Ver "Cómo configurar las políticas de actualización y de desinstalación de Symantec Management Agent" en la página 268.

Nota: Cuando instala Symantec Management Agent en un equipo, existe un retraso antes de que Client Task Agent se registre con Notification Server. Cualquier tarea que se realice en el equipo durante este tiempo (aproximadamente 10 minutos) tiene el estado pendiente hasta que Client Task Agent se registre. Cuando se registra Client Task Agent, las tareas se ejecutan de forma inmediata.

Instalar Symantec Management Agent en equipos con Windows

Es posible instalar Symantec Management Agent con una instalación manual en modo push o en modo pull. Se recomienda instalar Symantec Management Agent manualmente en modo push en los equipos seleccionados. Sin embargo, para realizar instalaciones en los equipos remotos con acceso limitado a la red o protegidos por un firewall, es posible que sea necesario realizar una instalación manual en modo pull.

Ver "Acerca de Symantec Management Agent" en la página 236.

Tabla 15-2 Proceso para instalar Symantec Management Agent en equipos con Windows

Paso	Acción	Descripción
Paso 1	Verifique que los equipos cumplan con los requisitos previos de instalación.	Cada equipo debe cumplir con los requisitos previos de hardware y software antes de instalar Symantec Management Agent. Ver "Requisitos previos de instalación de Symantec Management Agent para Windows" en la página 242.
Paso 2	(Opcional) Defina las políticas de registro de agentes.	Después de instalar Symantec Management Agent, envía una solicitud de registro a Notification Server para establecer una relación de confianza entre el servidor y el cliente. La política de registro de agentes predeterminada permite el registro automático de todos los agentes. Es posible modificar la política predeterminada o crear políticas personalizadas para especificar reglas más restrictivas. Ver "Crear una política de registro de agente" en la página 243.
Paso 3	Especifique la configuración de la instalación.	Antes de realizar la instalación manual en modo push o en modo pull de Symantec Management Agent, es necesario especificar la configuración de instalación. Ver "Especificar Symantec Management Agent para la configuración de instalación de Windows" en la página 245.
Paso 4	Instale Symantec Management Agent usando el método apropiado.	El método preferido es instalar Symantec Management Agent en modo push en los equipos seleccionados. No obstante, si algunos equipos se encuentran protegidos por un firewall o Notification Server tiene dificultades para acceder a ellos, es posible instalar Symantec Management Agent en modo pull en esos equipos. Ver "Cómo instalar Symantec Management Agent para Windows manualmente en modo push" en la página 246. Ver "Cómo instalar Symantec Management Agent para Windows con instalación manual en modo pull" en la página 247. Ver "Realizar una instalación programada de Symantec Management Agent para Windows" en la página 249.
Paso 5	Consulte el informe de estado de la instalación para verificar la instalación correcta.	El informe de estado de la instalación permite ver los detalles de todas las instalaciones manuales en modo push y las instalaciones programadas de Symantec Management Agent que se ha intentado llevar a cabo. El informe no incluye detalles de instalaciones remotas. Ver "Visualización del informe de estado de la instalación" en la página 250.

Paso	Acción	Descripción
Paso 6	Vea y administre el estado de registro del agente para verificar el registro correcto.	El informe **Estado de registro del agente** le permite ver y administrar todas las solicitudes de registro y los registros completos de los Symantec Management Agents. Ver "Ver y administrar el estado de registro del agente" en la página 251.

Requisitos previos de instalación de Symantec Management Agent para Windows

Antes de que pueda instalar Symantec Management Agent, es necesario configurar los equipos y verificar que cumplan con los requisitos previos de instalación.

Ver "Métodos para instalar Symantec Management Agent" en la página 238.

Esta tarea es un paso en los procesos para instalar Symantec Management Agent manualmente en equipos con Windows.

Ver "Instalar Symantec Management Agent en equipos con Windows" en la página 240.

Tabla 15-3 Requisitos previos de instalación de Symantec Management Agent para Windows

Requisito previo	Descripción
Sistema operativo	Cualquiera de los siguientes: ■ Windows 2003 SP2 (x86, x64) ■ Windows 2003 R2 y superior (x86, x64) ■ Windows XP Professional SP2 (x64) ■ Windows XP Professional SP3 (x86) ■ Windows Vista SP2 y superior (x86, x64) ■ Windows 2008 y superior (x86, x64) ■ Windows 2008 R2 y superior (x86, x64) ■ Windows 7 y superior (x86, x64)
Espacio en el disco duro	60 MB mínimo
RAM	64 MB mínimo (128 MB recomendado)
Internet Explorer	Versión 6.0 o posterior
Derechos de acceso	Derechos de administrador local

Requisito previo	Descripción
Firewall	El equipo debe poder comunicarse con Symantec Management Platform mediante el firewall del equipo. Realice alguna de las acciones siguientes: ■ Habilite **Uso compartido de archivos e impresoras** en la configuración del firewall. ■ Agregue los puertos UDP 138, TCP 445, TCP 80 (o TCP 443 para HTTPS) y el tipo 8 de ICMP como excepciones de puertos de entrada. Es posible agregar los puertos usando una política de grupo. ■ Desactive el firewall.
Uso compartido de archivos simple (Windows XP que no es de dominio solamente)	Para los equipos cliente que no son de dominio y ejecutan Windows XP, se debe además deshabilitar **Uso compartido de archivos simple**, en **Opciones de carpeta** en Windows XP.
UAC (Windows Vista y Windows 7 que no son de dominio solamente)	Para los equipos cliente que no son de dominio y ejecutan Windows Vista o Windows 7, se debe además desactivar el control de acceso de usuario (UAC).

Crear una política de registro de agente

Las políticas de registro de agente le permiten automatizar el proceso de registro del agente. Una política de registro de agente es un conjunto de reglas que determinan cómo se procesan las solicitudes de registro entrantes. En el contenido de la solicitud de registro, Symantec Management Agent envía su nombre de host, dirección MAC, dirección IP, FQDN y datos de usuarios conectados. La política de registro de agente usa los datos de la solicitud de registro y las reglas que se definen dentro de la política para decidir si la solicitud se permite o se bloquea.

Advertencia: La política de registro de agente predeterminada permite de forma automática que todos los agentes se comuniquen con Notification Server. Es posible modificar la política predeterminada o crear políticas personalizadas para restringir los agentes que se pueden comunicar con Notification Server. Si ninguna política activas está disponible, el estado de cada solicitud de registro entrante se configura como pendiente.

Es posible ver las solicitudes de registro en el informe de **Estado de registro del agente**. Es posible acceder a este informe en Symantec Management Console, en **Informes > Administración de Notification Server > Registro**.

Ver "Ver y administrar el estado de registro del agente" en la página 251.

Esta tarea es un paso opcional en los procesos siguientes:

- Instalar Symantec Management Agent en equipos con Windows.
  Ver "Instalar Symantec Management Agent en equipos con Windows" en la página 240.
- Instalar Symantec Management Agent manualmente en equipos con UNIX, Linux y Mac.
  Ver "Instalar Symantec Management Agent manualmente en equipos con UNIX, Linux y Mac" en la página 255.

Para crear una política de registro de agente

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Todas las configuraciones**.
2. En el panel izquierdo, en **Configuración**, expanda **Agentes/complementos > Symantec Management Agent > Configuración**.
3. Haga clic con el botón derecho en **Políticas de registro** y, después, haga clic en **Nueva > Política de registro**.
4. En el panel derecho, especifique la configuración de la política de registro de agente de la siguiente manera:

Reglas

Le permite definir diversos tipos de máscaras para identificación de agentes usando los datos de la solicitud. Por ejemplo, puede definir una máscara del nombre de host, una máscara de la dirección IP y una máscara del nombre de usuario conectado.

Una única política puede contener un número ilimitado de máscaras de cualquier tipo. Durante el proceso de coincidencia de máscaras, Notification Server toma los tipos diferentes de máscaras como operaciones AND lógicas y los tipos similares de máscaras como operaciones OR lógicas.

Por ejemplo, una política con las máscaras siguientes permite el registro de todos los agentes cuyo nombre coincide con la máscara "*prueba" y su dirección IP es 10.31.12.1, 10.31.12.2 o cualquiera de las 255 direcciones IP de la subred 10.31.15.0:

- Host = *prueba
- IP = 10.31.12.1
- IP = 10.31.12.2
- IP = 10.31.15.0/24

Nota: El asterisco se acepta para todas las reglas excepto para la **Dirección IP**. Si desea especificar un intervalo de IP en una regla, se debe definirla con la máscara de subred. Por ejemplo, en vez de escribir **10.31.15.***, escribe **10.31.15.0/24**.

Acciones	Le permite definir la regla para el procesamiento del agente correcto con las siguientes opciones: ■ **Permitir** Los agentes se registran de forma automática y no necesita aceptarlos manualmente. ■ **Bloquear** Las solicitudes de estos agentes se rechazan. Tenga en cuenta que si dos políticas son aplicables a una solicitud de registro, y una de ellas permite el registro y la otra lo bloquea, se aplica la política de bloqueo a la solicitud.

5 Active la política.

En la parte superior derecha de la página, haga clic en el círculo coloreado y, después, en **Activar**.

6 Haga clic en **Guardar cambios**.

Especificar Symantec Management Agent para la configuración de instalación de Windows

La configuración de instalación le permite especificar la forma de instalar Symantec Management Agent en el equipo cliente. Es posible configurar las opciones de instalación manual en modo push o en modo pull de Symantec Management Agent. Tenga en cuenta que no se puede incluir esta configuración en un archivo CSV cuando se importan nombres de equipos.

Esta tarea es un paso en los procesos para instalar Symantec Management Agent en equipos con Windows.

Ver "Instalar Symantec Management Agent en equipos con Windows" en la página 240.

Para configurar las opciones de instalación de Symantec Management Agent para Windows

1 En **Symantec Management Console**, en el menú **Acciones**, haga clic en **Agentes/complementos > Instalar automáticamente Symantec Management Agent**.

2 En la página **Instalación de Symantec Management Agent**, en **Instalación distribuida del agente en los equipos**, haga clic en **Configuración**.

3 En el cuadro de diálogo **Opciones de instalación de Symantec Management Agent**, seleccione las opciones que desee utilizar y especifique la configuración necesaria en los cuadros correspondientes. Luego, haga clic en **Aceptar**.

Para obtener más información, haga clic en la página y después presione **F1**.

4 En la página **Instalación de Symantec Management Agent**, haga clic en **Guardar cambios**.

Cómo instalar Symantec Management Agent para Windows manualmente en modo push

Es posible transferir Symantec Management Agent a cualquier equipo con Windows. Antes de que pueda instalar o desinstalar manualmente Symantec Management Agent desde la página **Instalación de Symantec Management Agent**, es necesario seleccionar los equipos de destino. Puede escribir los nombres de los equipos manualmente, elegir los equipos que se han detectado con la detección de recursos o importar los equipos desde un archivo CSV. El archivo CSV es un archivo de texto delimitado por comas. El archivo incluye los nombres de DNS o las direcciones IP de los equipos cliente en los cuales desea instalar Symantec Management Agent. Para equipos con Windows, el archivo CSV es una lista de nombres de equipos o direcciones IP que se importan en la página **Instalación de Symantec Management Agent**. Los elementos se interpretan como nombres de equipos o direcciones IP de equipos (para las entradas que están en el formato apropiado). Los espacios no están permitidos: se omite cualquier elemento que contenga un espacio.

Nota: Usted puede instalar manualmente Symantec Management Agent solamente en los equipos que fueron detectados usando **Detección de recursos de dominio** o **Network Discovery**.

Esta tarea es un paso en los procesos para instalar Symantec Management Agent en equipos con Windows.

Ver "Instalar Symantec Management Agent en equipos con Windows" en la página 240.

Para instalar Symantec Management Agent para Windows manualmente en modo push

1 En Symantec Management Console, en el menú **Acciones**, haga clic en **Agentes/complementos > Instalar automáticamente Symantec Management Agent**.

2 En la página de **Instalación de Symantec Management Agent**, en la ficha **Instalar el agente**, en **Instalación distribuida del agente en los equipos**,

elija los equipos en los cuales desea instalar Symantec Management Agent y después haga clic en **Instalar**.

Para agregar un equipo de forma manual	En el cuadro de texto, escriba el nombre del equipo (que debe ser un nombre que se puede resolver por DNS) o dirección IP y, a continuación, haga clic en **Agregar**.
Para elegir entre los equipos disponibles	1 Haga clic en **Seleccionar equipos**. 2 En el cuadro de diálogo **Seleccionar equipos**, agregue los equipos apropiados de la lista **Equipos disponibles** a la lista **Equipos seleccionados** y después haga clic en **Aceptar**.
Para importar equipos a partir de un archivo CSV	1 En **Instalación distribuida del agente en los equipos**, en la barra de herramientas, haga clic en el símbolo **Importar los equipos desde un archivo seleccionado**. 2 En el cuadro de diálogo **Seleccionar archivo para importar**, seleccione el archivo CSV apropiado y, luego, haga clic en **Abrir**.

3 En el cuadro de diálogo **Opciones de instalación de Symantec Management Agent**, establezca la configuración de instalación según sus necesidades y después haga clic en **Proceder con la instalación**.

Para obtener más información, haga clic en la página y después presione **F1**.

En la página **Instalación de Symantec Management Agent**, en **Instalación distribuida del agente en los equipos**, en la lista de equipos, la columna **Estado** muestra el resultado correcto o con error de la instalación en cada equipo. Tenga en cuenta que el Symantec Management Agent recién instalado vuelve a informar su estado al Notification Server de origen, incluso si va a ser administrado por otro Notification Server.

Cómo instalar Symantec Management Agent para Windows con instalación manual en modo pull

Si se desea instalar Symantec Management Agent en equipos remotos con acceso limitado a la red o protegidos por un firewall, es posible que sea necesario instalar Symantec Management Agent con instalación remota, en cada equipo. Es posible iniciar sesión en cada equipo, acceder a Notification Server con una URL e iniciar el proceso de instalación de Symantec Management Agent. El proceso de instalación se ejecuta automáticamente y no requiere mayor interacción con el usuario.

Ver "Acerca de Symantec Management Agent" en la página 236.

La instalación remota de Symantec Management Agent usa la configuración que se especifica en el cuadro de diálogo **Opciones de instalación de Symantec Management Agent**, a excepción de **Descargar el paquete del agente desde el agente de Package Server más cercano** que no es relevante.

La URL de la página **Descarga de Symantec Management Agent** se muestra en la página **Instalación de Symantec Management Agent**, en **URL de página de descarga**. Esta configuración no se puede modificar.

Esta tarea es un paso en los procesos para instalar Symantec Management Agent en equipos con Windows.

Ver "Instalar Symantec Management Agent en equipos con Windows" en la página 240.

Para ver previamente la página Descarga del kit de Symantec Management Agent

1. En Symantec Management Console, en el menú **Acciones**, haga clic en **Agentes/complementos > Instalar automáticamente Symantec Management Agent**.
2. En la página **Instalación de Symantec Management Agent**, bajo **URL de página de descarga**, haga clic en **Mostrar esta página**.

Para instalar Symantec Management Agent para Windows con instalación remota manual

1. Inicie sesión en el equipo como administrador.

   Se puede iniciar sesión de forma remota, con una aplicación de acceso remoto como pcAnywhere, o se puede permitir a un usuario del sitio remoto iniciar sesión con la cuenta apropiada.
2. En el equipo remoto, abra Internet Explorer y vaya a la siguiente dirección URL:

   http://*NSName*/Altiris/NS/Agent/AltirisAgentDownload.aspx

   donde *NSName* es el nombre de su equipo con Notification Server.
3. En la ventana **Descarga de Symantec Management Agent**, haga clic en **Haga clic aquí para empezar la descarga y la instalación**.

   El proceso de instalación del agente se ejecuta silenciosamente y no requiere mayor intervención.

Realizar una instalación programada de Symantec Management Agent para Windows

Es posible configurar una instalación programada de Symantec Management Agent. Una instalación programada se realiza en un momento definido, a diferencia de las instalaciones push manuales que se realizan de forma inmediata. Por ejemplo, si desea instalar el agente en un grupo determinado de equipos en un momento conveniente, puede configurar una programación sin repetición para que se ejecute en el momento apropiado.

Puede además configurar una programación para instalar automáticamente Symantec Management Agent en nuevos equipos a medida que se agregan a su entorno. La programación de detección de recursos se ejecuta diariamente para detectar nuevos equipos, y puede configurar filtros para ordenar los nuevos equipos en los grupos apropiados. Luego, puede programar la instalación de Symantec Management Agent en todos los equipos de determinados grupos en los intervalos apropiados.

Es necesario tener cuidado al implementar un método de instalación automática; recomendamos incluir un paso manual para verificar que el agente se instale en los equipos apropiados.

Esta tarea es un paso en los procesos para instalar Symantec Management Agent en equipos con Windows.

Ver "Instalar Symantec Management Agent en equipos con Windows" en la página 240.

Para configurar la programación de instalación de Symantec Management Agent para Windows

1. En **Symantec Management Console**, en el menú **Acciones**, haga clic en **Agentes/complementos > Instalar automáticamente Symantec Management Agent**.
2. En la página **Instalación de Symantec Management Agent**, en **Instalación automática programada en los equipos**, a la derecha de la página, haga clic en el círculo coloreado y después haga clic en **Activado**.
3. En **Aplicar a**, especifique los equipos en los cuales se debe instalar Symantec Management Agent.

   Puede especificar un grupo organizativo, un filtro o un destino de recursos existente. También puede seleccionar recursos individuales.

   Ver "Especificación de destinos de una política o tarea" en la página 379.

4 En el panel **Cuándo programar**, especifique la hora programada o la ventana de programación para realizar la instalación y seleccione las opciones apropiadas.

5 Haga clic en **Guardar cambios**.

Visualización del informe de estado de la instalación

El informe de estado de la instalación permite ver los detalles de todos los intentos de instalación push de Symantec Management Agent que se han hecho. El informe no incluye detalles de instalaciones remotas.

De forma predeterminada, se enumeran los detalles de todos los intentos de instalación realizados en la última semana. Es posible especificar el período para ver y filtrar los resultados por nombre del equipo y el dominio.

Esta tarea es un paso en los procesos siguientes:

- Instalar Symantec Management Agent en equipos con Windows.
  Ver "Instalar Symantec Management Agent en equipos con Windows" en la página 240.
- Instalar Symantec Management Agent manualmente en equipos con UNIX, Linux y Mac.
  Ver "Instalar Symantec Management Agent manualmente en equipos con UNIX, Linux y Mac" en la página 255.

Para ver el informe Estado de instalación del agente

1 En Symantec Management Console, en el menú **Acciones**, haga clic en **Agentes/complementos > Instalar automáticamente Symantec Management Agent**.

2 En la página **Instalación de Symantec Management Agent**, haga clic en **Informe de estado**.

El informe muestra los detalles de todos los intentos de la instalación push para Symantec Management Agent y Symantec Management Agent para UNIX, Linux y Mac. El mismo informe está disponible en las fichas **Instalar el agente** e **Instalar agente para UNIX, Linux y Mac**.

3 En la ventana **Estado de instalación del agente**, consulte los detalles de cada intento de instalación.

4 (Opcional) Si desea cambiar el período o filtrar los resultados por nombre de equipo y dominio, bajo **Parámetros**, configure los parámetros de usuario apropiados:

Mostrando...	Especifique el período que desea ver. Escriba el número de unidades apropiado (horas, días, semanas o meses) en los cuadros **Desde** y **Hasta**.
Unidades	Especifique las unidades que desee usar para los valores de **Mostrando**.
Filtrar por	Si desea filtrar los resultados por nombre de equipo o dominio (o ambos), especifique el texto apropiado del filtro en los cuadros correspondientes.

5 (Opcional) Si ha cambiado los parámetros de usuario, haga clic en **Actualizar** para visualizar los resultados actualizados del informe.

Ver y administrar el estado de registro del agente

El informe de **Estado de registro del agente** le permite ver todas las solicitudes de registro y los registros completos de los Symantec Management Agents.

En este informe, puede ver los equipos que la **Política de registro de agente** ha permitido o bloqueado de forma automática. Tenga en cuenta que para la instalación push directa de Symantec Management Agent, el registro se omite. Sin embargo, los equipos aún se muestran en el informe y el estado se configura como **Permitido**. Si ninguna **Política de registro de agente** se aplica al equipo, el estado se configura en **Pendiente** y el menú contextual le permite permitirlo o bloquearlo manualmente. El menú contextual además le permite revocar la confianza de los agentes que tiene previamente permitidos.

Ver "Crear una política de registro de agente" en la página 243.

Las solicitudes de registro entrantes se distinguen por las claves de recursos y se combinan en función de la búsqueda de claves de recursos.

En algunas situaciones, pueden aparecer solicitudes de registro duplicadas. Por ejemplo, si reinstala el agente en un equipo que ya está registrado en Notification Server, la clave pública cambia. En este caso, Symantec recomienda que autorice la solicitud de registro para permitir que este equipo continúe comunicándose con Notification Server. Además, pueden aparecer solicitudes de registro duplicadas si tiene equipos con las claves idénticas de recursos en la red. En este caso, Symantec recomienda no autorizar la solicitud de registro duplicada, porque puede causar problemas de conectividad para el recurso que existió previamente.

Si tiene solicitudes de registro duplicadas en el informe, las solicitudes se administran de la siguiente manera:

- Si la solicitud inicial está permitida y la solicitud duplicada también está permitida, la solicitud duplicada se combina con el recurso existente y el informe se actualiza para mostrar una única entrada.
- Si la solicitud inicial está permita pero la solicitud duplicada está bloqueada, ambas solicitudes permanecen en la lista. La solicitud permitida representa al recurso real y la solicitud duplicada en estado bloqueado o pendiente representa el intento del registro de un recurso potencialmente duplicado.

El informe de **Estado de registro del agente** guarda todas las solicitudes con fines de auditoría y le permite observarlos continuamente.

Esta tarea es un paso en los procesos siguientes:

- Instalar Symantec Management Agent en equipos con Windows.
  Ver "Instalar Symantec Management Agent en equipos con Windows" en la página 240.
- Instalar Symantec Management Agent manualmente en equipos con UNIX, Linux y Mac.
  Ver "Instalar Symantec Management Agent manualmente en equipos con UNIX, Linux y Mac" en la página 255.

Para ver y administrar el estado de registro del agente

1. En Symantec Management Console, en el menú **Informes**, haga clic en **Todos los informes**.
2. En el panel izquierdo, en **Informes**, expanda **Administración de Notification Server > Registro** y, después, haga clic en **Estado de registro del agente**.

3 (Opcional) En la página **Estado de registro del agente**, use las opciones del menú contextual de modificar el estado del agente. Tenga en cuenta que según el estado del agente, las opciones del menú contextual varían.

Permitir

Es posible permitir los agentes que están en estado **Pendiente**, **Bloqueado** o **Revocado**.

Si permite un agente bloqueado, la confianza se concede la vez próxima que el agente envía una solicitud de registro a Notification Server.

Bloquear

Es posible bloquear los agentes que están en estado **Pendiente** o **Revocado**.

Si bloquea un equipo revocado, el estado funcional no cambia. Sin embargo, cambiar el estado le permite distinguir los equipos revocados que nunca más deben conectarse a Notification Server desde los equipos revocados que pueden aún requerir su atención.

Tenga en cuenta que los equipos con el estado **Bloqueado** se eliminan de la lista después de un período predefinido si no se enviaron nuevas solicitudes de registro desde el mismo equipo durante este tiempo. El período predeterminado es de tres meses, pero puede cambiarlo en la página **Mantenimiento de depuración**.

Revocar

Es posible revocar el registro de los agentes que tiene previamente permitidos. Por ejemplo, puede revocar el registro del equipo cliente informado como extraviado o robado. Después de revocar el agente, este deja de recibir políticas de Notification Server. Además, un equipo revocado no se puede usar como servidor de sitio.

Durante la revocación de la confianza interna del agente, el registro de la clave de cifrado del agente se marca como revocado en Notification Server. Los agentes revocados no reciben políticas y no ejecutan tareas. Además, el agente revocado borra las políticas almacenadas localmente para reducir al mínimo la actividad. Después de la revocación, Symantec Management Agent debe reiniciar obligatoriamente el proceso de registro.

El agente recibe la información sobre el estado revocado la próxima vez que intenta acceder a los datos protegidos. Notification Server no notifica al agente sobre el evento de revocación cuando ocurre.

Tenga en cuenta que el agente revocado sigue en estado **Revocado** incluso si la política de registro de agente lo permite. Es necesario administrar manualmente los equipos revocados si desea cambiar el estado.

Instalar Symantec Management Agent manualmente en equipos con UNIX, Linux y Mac

Es posible instalar Symantec Management Agent con una instalación manual en modo push o en modo pull. Se recomienda instalar Symantec Management Agent manualmente en modo push en los equipos seleccionados. Sin embargo, para realizar instalaciones en los equipos remotos con acceso limitado a la red o protegidos por un firewall, es posible que sea necesario realizar una instalación manual en modo pull.

Ver "Acerca de Symantec Management Agent" en la página 236.

Tabla 15-4 Proceso para instalar Symantec Management Agent manualmente en los equipos con UNIX, Linux y Mac

Paso	Acción	Descripción
Paso 1	Seleccione los equipos en los cuales desea instalar el agente y los complementos.	Tiene las siguientes opciones para seleccionar equipos: ■ Network Discovery ■ Selección manual agregando direcciones IP o nombres de host de cliente ■ Importación de Active Directory ■ Importación mediante un archivo de valores separados por coma.
Paso 2	Verifique que los equipos cumplan con los requisitos previos de instalación.	Cada equipo debe cumplir con los requisitos previos de hardware y software antes de instalar Symantec Management Agent. Ver "Requisitos previos para la instalación de Symantec Management Agent para UNIX, Linux y Mac" en la página 258.
Paso 3	(Opcional) Defina las políticas de registro de agentes.	Después de instalar Symantec Management Agent, envía una solicitud de registro a Notification Server para establecer una relación de confianza entre el servidor y el cliente. La política de registro de agentes predeterminada permite el registro automático de todos los agentes. Es posible modificar la política predeterminada o crear políticas personalizadas para especificar reglas más restrictivas. Ver "Crear una política de registro de agente" en la página 243.

Paso	Acción	Descripción
Paso 4	Especifique la configuración de la instalación.	La configuración de instalación de UNIX, Linux y Mac permite configurar las opciones de comunicación y autenticación de Symantec Management Agent para UNIX, Linux y Mac. Si se importan nombres de equipos desde un archivo CSV, es posible especificar estas opciones en ese archivo. También es posible establecer o modificar estas opciones de configuración desde Symantec Management Console. Ver "Cómo especificar la configuración de instalación de Symantec Management Agent para UNIX, Linux y Mac " en la página 259.
Paso 5	Instale Symantec Management Agent usando el método apropiado.	El método preferido es instalar Symantec Management Agent en modo push en los equipos seleccionados. No obstante, si algunos equipos se encuentran protegidos por un firewall o Notification Server tiene dificultades para acceder a ellos, es posible instalar Symantec Management Agent en modo pull en esos equipos. Ver "Cómo instalar Symantec Management Agent para UNIX, Linux y Mac manualmente en modo push" en la página 260. Ver "Cómo instalar Symantec Management Agent para UNIX, Linux y Mac manualmente en modo pull" en la página 264.
Paso 6	Vea y administre el estado del registro del agente para verificar que el registro se haya realizado correctamente.	El informe **Estado de registro del agente** le permite ver y administrar todas las solicitudes de registro y los registros completados de los Symantec Management Agents. Ver "Ver y administrar el estado de registro del agente" en la página 251.

Cómo crear un archivo CSV para importar equipos con UNIX, Linux y Mac

Si se desea instalar Symantec Management Agent para UNIX, Linux y Mac en una gran cantidad de equipos que requieran opciones de configuración y conexión diferentes, se recomienda usar un archivo CSV para importar los equipos y determinar la configuración de instalación. El archivo CSV es un archivo de texto delimitado por comas que incluye los nombres DNS o las direcciones IP de los equipos cliente en los cuales desea instalar Symantec Management Agent. Cada línea del archivo CSV representa la entrada de un equipo que se importa en la página **Instalación de Symantec Management Agent**. El archivo CSV también puede incluir la configuración de instalación para cada equipo.

Ver "Cómo instalar Symantec Management Agent para UNIX, Linux y Mac manualmente en modo push" en la página 260.

Symantec Management Platform proporciona un archivo de plantilla CSV para importar equipos con UNIX, Linux y Mac (`CSVTemplate.csv`). El encabezado de la columna de la plantilla CSV indica los datos que son necesarios y los valores válidos que se pueden usar.

Advertencia: El formato de archivo CSV (separador de lista) debe coincidir con la configuración regional del servidor. Por ejemplo, el archivo de muestra `CSVTemplate.csv` utiliza la configuración regional "Inglés (Estados Unidos)" con una coma "," como separador de lista. Es posible ver la configuración regional de Symantec Management Platform en el **Panel de control** de Windows.

Esta tarea es un paso en el proceso para instalar Symantec Management Agent manualmente.

Ver "Instalar Symantec Management Agent en equipos con Windows" en la página 240.

Para crear un archivo CSV para importar equipos con UNIX, Linux y Mac

1. En Symantec Management Console, en el menú **Acciones**, haga clic en **Agentes/complementos > Instalar automáticamente Symantec Management Agent**.
2. En la página **Instalación de Symantec Management Agent**, en la ficha **Instalación del agente para UNIX, Linux y Mac**, en **Realizar la instalación distribuida del agente para UNIX, Linux y Mac en los equipos**, haga clic con el botón derecho en **Plantilla del archivo CSV** y, después, haga clic en **Guardar destino como**.
3. En el cuadro de diálogo **Guardar como**, escriba un nombre de archivo conveniente para el archivo `CSVTemplate.csv`, vaya a la ubicación apropiada y, después, haga clic en **Guardar**.
4. Abra el archivo CSV guardado en un editor de texto y escriba la información de cada equipo en el cual desee instalar Symantec Management Agent para UNIX, Linux y Mac.

   No es necesario que utilice todos los campos. Puede utilizar solamente los campos que necesite, como nombre del equipo, nombre de raíz, contraseña de raíz, etc.

   Las opciones de configuración que se pueden especificar en el archivo CSV son las mismas que se pueden determinar desde la ventana **Configuración de instalación** en Symantec Management Console.
5. Una vez finalizado el proceso, guarde el archivo CSV.

Requisitos previos para la instalación de Symantec Management Agent para UNIX, Linux y Mac

El equipo debe cumplir con los requisitos previos de hardware y software para poder instalar Symantec Management Agent para UNIX, Linux y Mac.

Ver "Métodos para instalar Symantec Management Agent" en la página 238.

Este tema es un paso en el proceso para instalar Symantec Management Agent manualmente.

Ver "Instalar Symantec Management Agent en equipos con Windows" en la página 240.

Tabla 15-5 Requisitos previos para la instalación de Symantec Management Agent para UNIX, Linux y Mac

Requisito previo	Descripción
Sistema operativo	Cualquiera de los siguientes sistemas operativos: ■ Solaris 9 (SPARC) ■ Solaris 10 (x86, x86_64 y SPARC) ■ Red Hat Enterprise Linux 5.0, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 5.8, 5.9 (x86 y x86_64) ■ Red Hat Enterprise Linux 6.0, 6.1, 6.2, 6.3, 6.4 (x86 y x86_64) ■ SUSE Linux Enterprise Server 10, 11 SP1, 11 SP2 (x86 y x86_64) ■ SUSE Linux Enterprise Desktop 10, 11 SP1, 11 SP2 (x86 y x86_64) ■ Mac OS X 10.6.x, 10.7.x, 10.8.x (binario universal) ■ Servidor Mac OS X 10.6.x, 10.7.x, 10.8.x (binario universal) ■ HP-UX 11.11 (PA-RISC), 11.23 (PA-RISC/IA64), 11.31 (PA-RISC/IA64) ■ AIX 6.1 PPC, 7.1 Standard
Espacio en el disco duro	60 MB mínimo
RAM	25 MB mínimo
Derechos de acceso	Los derechos de acceso del usuario raíz son necesarios en todas las plataformas de UNIX/Linux. Para Mac OS X administrativo o usuario raíz, se necesitan derechos de acceso.

Requisito previo	Descripción
Conexiones remotas SSH habilitadas	Las conexiones remotas SSH deben estar habilitadas. El equipo cliente debe poseer un servidor SSH en ejecución y la configuración del firewall debe admitir una conexión entrante SSH.
Conexión saliente a Notification Server habilitada.	La configuración del firewall debe admitir una conexión saliente a un puerto WEB en Notification Server.

Cómo especificar la configuración de instalación de Symantec Management Agent para UNIX, Linux y Mac

La configuración de instalación de Symantec Management Agent es la configuración de comunicación y de autenticación de Symantec Management Agent para UNIX, Linux y Mac. Es necesario especificar el nombre de inicio de sesión y la contraseña de la cuenta con privilegios correcta para cada equipo de destino.

Ver "Cómo instalar Symantec Management Agent para UNIX, Linux y Mac manualmente en modo push" en la página 260.

Cuando se importan equipos de un archivo CSV, es posible especificar la configuración de instalación adecuada para cada equipo en el archivo CSV. Si no se especifica ninguna configuración en el archivo CSV, o si los equipos se agregaron de forma manual, es necesario especificar la configuración adecuada para cada equipo de destino antes de instalar Symantec Management Agent para UNIX, Linux y Mac.

Es posible especificar la configuración de instalación para un equipo determinado o para varios equipos. Si selecciona varios equipos, se aplica la misma configuración de instalación a cada equipo. También es posible clonar la configuración de instalación actual de un equipo y aplicarla a otros equipos.

Ver "Cómo crear un archivo CSV para importar equipos con UNIX, Linux y Mac" en la página 256.

Esta tarea es un paso en el proceso para instalar Symantec Management Agent manualmente.

Ver "Instalar Symantec Management Agent en equipos con Windows" en la página 240.

Para especificar Symantec Management Agent para la configuración de instalación de UNIX, Linux y Mac

1. En Symantec Management Console, en el menú **Acciones**, haga clic en **Agentes/complementos > Instalar automáticamente Symantec Management Agent**.
2. En la página **Instalación de Symantec Management Agent**, en la ficha **Instalación del agente para UNIX, Linux y Mac**, en **Realizar la instalación distribuida del agente para UNIX, Linux y Mac en los equipos**, en la lista de equipos, haga clic en el equipo para el cual desee cambiar la configuración de instalación de Symantec Management Agent y, después, haga clic en **Configuración de instalación**.

   Si desea especificar configuraciones de instalación idénticas para varios equipos o si desea clonar la configuración de instalación actual desde otro equipo, seleccione los equipos apropiados.
3. (Opcional) Si desea clonar la configuración de instalación actual de un equipo determinado, en el cuadro de diálogo **Configuración de instalación** de la lista desplegable **Cargar configuración**, seleccione el equipo apropiado.

   La opción **Cargar configuración de** aparece a la derecha de la parte superior del cuadro de diálogo **Configuración de instalación** si ha seleccionado varios equipos.
4. Especifique la configuración de instalación adecuada para los equipos seleccionados.

   Para obtener más información, haga clic en la página y, después, presione **F1**.
5. En el cuadro de diálogo **Configuración de instalación**, haga clic en **Aceptar**.

Cómo instalar Symantec Management Agent para UNIX, Linux y Mac manualmente en modo push

Es posible instalar en modo push Symantec Management Agent para UNIX, Linux y Mac en cualquiera de los equipos que se enumeran en la página Instalación de Symantec Management Agent.

Antes de que pueda instalar o desinstalar manualmente Symantec Management Agent desde la página **Instalación de Symantec Management Agent**, es necesario seleccionar los equipos apropiados. Puede seleccionar los equipos que se han detectado con la detección de recursos, escribir los nombres de los equipos manualmente o importar los equipos a partir de un archivo CSV.

Nota: Usted puede instalar manualmente Symantec Management Agent solamente en los equipos que fueron detectados usando **Detección de recursos de dominio** o **Network Discovery**.

La instalación en modo push de Symantec Management Agent para UNIX, Linux y Mac la realiza el equipo con Symantec Management Platform. El equipo de Symantec Management Platform establece una conexión con el equipo UNIX, Linux o Mac de destino, carga los archivos necesarios y los ejecuta en el equipo de destino.

El proceso de instalación es el siguiente:

- La Plataforma de administración Symantec intenta conectarse con el equipo de destino a través de SSH.
  El protocolo SSH admite el inicio de sesión con cuentas de usuario no autorizado o cuentas con privilegios y varias contraseñas.
- Una vez que se establece la conexión, Symantec Management Platform determina el entorno y el sistema operativo del equipo cliente. A continuación, inicia el script de instalación remota adecuado para la plataforma específica.
- El script de instalación remota genera una estructura de directorios en el equipo cliente e intenta descargar la utilidad `aex-bootstrap` del equipo con Symantec Management Platform. El script de instalación automática prueba, en orden, cada uno de los siguientes métodos hasta que uno da resultado: SCP/SFTP, wget, curl.
  Si ninguno de estos métodos funciona, el script usa el comando "dd" para transferir el archivo aex-bootstrap.Z.uu al equipo de destino. Luego usa el código "uu" para convertir el archivo a un formato nativo.
- El archivo `.aex-agent-install-config.xml` que contiene toda la configuración de instalación de Symantec Management Agent se descarga en el equipo cliente.
- El script `aex-bootstrap` se ejecuta y se cierra la conexión con Symantec Management Platform.
- El script `aex-bootstrap` descarga el resto de Symantec Management Agent del equipo con Symantec Management Platform y configura Symantec Management Agent con valores de configuración del archivo `.aex-agent-install-config.xml`.
- Cuando Symantec Management Agent para UNIX, Linux y Mac se ejecuta por primera vez, recopila el inventario básico y lo envía a Symantec Management Platform.

- Symantec Management Agent para UNIX, Linux y Mac recibe las tareas y las políticas adecuadas de Symantec Management Platform.

Nota: Los firewalls de otro fabricante se deben configurar para permitir una conexión SSH de Symantec Management Platform al cliente ULM para que funcione una instalación manual en modo push. Los firewalls de configuración deben usar las mismas credenciales que usted proporcionó en el cuadro de diálogo **Configuración de instalación** en el paso 4.

Esta tarea es un paso en el proceso para instalar Symantec Management Agent manualmente.

Ver "Instalar Symantec Management Agent en equipos con Windows" en la página 240.

Para instalar Symantec Management Agent para UNIX, Linux y Mac manualmente en modo push

1. En Symantec Management Console, en el menú **Acciones**, haga clic en **Agentes/complementos > Instalar automáticamente Symantec Management Agent**.
2. En la página **Instalación de Symantec Management Agent**, en la ficha **Instalar agente para UNIX, Linux y Mac**, en **Realizar la instalación distribuida del agente para UNIX, Linux y Mac en los equipos**, seleccione los equipos con UNIX, Linux y Mac en los cuales desea instalar Symantec Management Agent:

Para agregar un equipo de forma manual	En el cuadro de texto, escriba el nombre del equipo (que debe ser un nombre que se puede resolver por DNS) o dirección IP y, a continuación, haga clic en **Agregar**.
Para seleccionar desde los equipos disponibles	Haga clic en **Seleccionar equipos**, en el cuadro de diálogo **Seleccionar equipos**, agregue los equipos apropiados de la lista **Equipos disponibles** a la lista **Equipos seleccionados** y después haga clic en **Aceptar**.

Para importar equipos a partir de un archivo CSV

1 En la barra de herramientas, haga clic en **Importar los equipos desde un archivo seleccionado**.

2 En el cuadro de diálogo **Seleccionar archivo para importar**, seleccione el archivo CSV apropiado y, luego, haga clic en **Abrir**.

El archivo CSV es un archivo de texto delimitado por comas. El archivo incluye los nombres de DNS o las direcciones IP de los equipos cliente en los cuales desea instalar Symantec Management Agent. Para equipos con UNIX, Linux y Mac, cada línea en el archivo CSV representa la entrada de un equipo que se importa en la página **Instalación de Symantec Management Agent**. Es posible también incluir la configuración de instalación apropiada en el archivo CSV. Esta configuración de instalación permite configurar los valores de comunicación y autenticación de Symantec Management Agent para UNIX, Linux y Mac.

Si tiene un gran número de equipos que necesitan diversos valores de conexión y configuración, use un archivo CSV para importar los equipos.

Ver "Cómo crear un archivo CSV para importar equipos con UNIX, Linux y Mac" en la página 256.

3 Haga clic en **Configuración de instalación** y, a continuación, en el cuadro de diálogo **Configuración de instalación**, especifique la configuración de instalación apropiada.

Si ha agregado equipos de forma manual, debe especificar la configuración de instalación apropiada para cada equipo de destino antes de instalar Symantec Management Agent para UNIX, Linux y Mac. Si ha importado equipos a partir de archivo CSV, es posible que la configuración de instalación para cada equipo esté especificada en el archivo CSV. Puede modificar estas opciones para equipos individuales o grupos de equipos.

Ver "Cómo especificar la configuración de instalación de Symantec Management Agent para UNIX, Linux y Mac " en la página 259.

4 (Opcional) En el cuadro **Tareas simultáneas**, especifique la cantidad de instalaciones que se deben ejecutar en forma simultánea.

Este valor define la cantidad de subprocesos que se ejecutan paralelamente y participan en la instalación en modo push de Symantec Management Agent. Todos los subprocesos comparten una cola común de la cual toman el siguiente equipo para realizar la instalación. El valor predeterminado es 5, pero se puede usar un valor diferente que se adapte al rendimiento de Symantec Management Platform, los equipos cliente y la capacidad de la red. El aumento de la cantidad de tareas simultáneas puede reducir el tiempo de instalación total.

5 Haga clic en **Instalar**.

6 En el cuadro de diálogo **Instalación push**, seleccione la casilla para aceptar la instalación del software de otro fabricante y después haga clic en **Aceptar**.

Nota: Si la plataforma de destino es RHEL de 64 bits 6.0 o superior y no tiene capa de compatibilidad de 32 bits instalada, la instalación push del agente genera errores si usted no acepta la instalación del software de otro fabricante.

La columna **Estado** en la lista de equipos muestra el resultado correcto o incorrecto de la instalación en cada equipo. Tenga en cuenta que Symantec Management Agent recién instalado informa su estado al Notification Server que lo origina, incluso si otro Notification Server lo administra.

7 Si la lista de equipos no se actualiza automáticamente, haga clic en **Actualizar** en la barra de herramientas para ver el estado actual de la instalación push para cada equipo.

Cómo instalar Symantec Management Agent para UNIX, Linux y Mac manualmente en modo pull

Si SSH no está disponible o si desea instalar Symantec Management Agent para UNIX, Linux y Mac en equipos remotos que tienen acceso limitado a la red, o en equipos de destino que están protegidos por un firewall, se puede realizar la instalación remota de Symantec Management Agent en cada equipo. Cualquier persona con derechos de administrador, puede iniciar sesión en cada equipo, acceder a Symantec Management Platform por medio de una URL y descargar el programa de secuencia de arranque que realiza la instalación de Symantec Management Agent para UNIX, Linux y Mac.

La URL de la página **Descargar Symantec Management Agent para UNIX, Linux y Mac** se muestra en la página **Instalación de Symantec Management Agent**, en **URL de la página de descarga para UNIX, Linux y Mac**. Es posible ver la página, pero no se puede cambiar esta configuración.

Ver "Acerca de Symantec Management Agent" en la página 236.

Ver "Comandos de solución de problemas de Symantec Management Agent para UNIX, Linux y Mac" en la página 511.

Esta tarea es un paso en el proceso para instalar Symantec Management Agent manualmente.

Ver "Instalar Symantec Management Agent en equipos con Windows" en la página 240.

Para obtener una vista previa de la página Descargar Symantec Management Agent para UNIX, Linux y Mac

1. En Symantec Management Console, en el menú **Acciones**, haga clic en **Agentes/complementos > Instalar automáticamente Symantec Management Agent**.
2. En la página **Instalación de Symantec Management Agent**, en la ficha **Instalar Symantec Management Agent para UNIX, Linux y Mac**, en **URL de la página de descarga para usuarios de UNIX, Linux y Mac**, en la lista desplegable **Seleccionar plataforma**, haga clic en la plataforma apropiada y, después, haga clic en **Visualizar página**.

Para realizar la instalación remota de Symantec Management Agent para UNIX, Linux y Mac en un equipo remoto

1. Inicie sesión en el equipo remoto como administrador.
2. En el equipo remoto, abra un navegador web y después vaya a la siguiente URL:

   http://*NombredeSMP*/Altiris/UnixAgent/AltirisUnixAgentDownload.aspx?ID=*Plataforma*

   donde *NombredeSMP* es el nombre de su equipo con Symantec Management Platform y *Plataforma* es la plataforma apropiada.
3. Siga las instrucciones que se muestran en la página **Descargar Symantec Management Agent para UNIX, Linux y Mac** para descargar y ejecutar el programa de secuencia de arranque de instalación en el equipo remoto.

Capítulo 16

Actualizar y desinstalar Symantec Management Agent

En este capítulo se incluyen los temas siguientes:

- Métodos para actualizar Symantec Management Agent
- Métodos para desinstalar Symantec Management Agent
- Cómo configurar las políticas de actualización y de desinstalación de Symantec Management Agent
- Acerca de la comunicación de agente de una versión anterior
- Configuración del paquete de Symantec Management Agent
- Cómo quitar Symantec Management Agent para Windows manualmente

Métodos para actualizar Symantec Management Agent

Debe instalar la versión apropiada de Symantec Management Agent en los equipos administrados. Si los equipos tienen versiones anteriores del agente instaladas, debe actualizarlas.

Ver "Acerca de Symantec Management Agent" en la página 236.

Tabla 16-1 Métodos de actualización de Symantec Management Agent

Método	Descripción
Instalación push manual de Symantec Management Agent en los equipos apropiados.	Usted puede actualizar Symantec Management Agent instalándolo manualmente en los equipos apropiados. Puede realizar una instalación automática en un equipo que tenga instalada una versión anterior de Symantec Management Agent. Ver "Cómo instalar Symantec Management Agent para Windows manualmente en modo push" en la página 246. Ver "Cómo instalar Symantec Management Agent para UNIX, Linux y Mac manualmente en modo push" en la página 260.
Use la política de actualización de Symantec Management Agent.	La política de actualización de Symantec Management Agent se proporciona con Notification Server. Puede activar dicha política y configurarla a fin de garantizar que todos los equipos administrados tengan instalada la versión correcta de Symantec Management Agent. Ver "Cómo configurar las políticas de actualización y de desinstalación de Symantec Management Agent" en la página 268. **Nota:** Mientras realiza la transición de IT Management Suite de versiones anteriores a 7.5, el modo **Comunicación de agente de una versión anterior** (LACA) habilitado permite que un Notification Server actualizado realice un conjunto limitado de funciones de administración en endpoints con versiones anteriores de Symantec Management Agent. Es posible administrar el modo **Comunicación de agente de una versión anterior** en Symantec Management Console, en la ficha **Procesamiento** de la página **Valores de configuración de Notification Server**. Ver "Acerca de la comunicación de agente de una versión anterior" en la página 272. Ver "Cómo configurar los valores de Notification Server" en la página 68.

Métodos para desinstalar Symantec Management Agent

Puede eliminar Symantec Management Agent de los equipos administrados si ya no lo necesita. No necesita quitar ningún agente de solución que haya sido instalado

en el equipo, ya que se eliminan automáticamente como parte del proceso de desinstalación de Symantec Management Agent.

Ver "Acerca de Symantec Management Agent" en la página 236.

Tabla 16-2 Métodos para desinstalar Symantec Management Agent

Método	Descripción
Desinstalación manual.	La desinstalación manual se inicia en Symantec Management Console y elimina Symantec Management Agent de inmediato. Puede quitar Symantec Management Agent de cualquier cantidad de equipos con Windows en la misma operación de desinstalación. También puede actualizar las opciones de desinstalación para cada operación. Esta opción está disponible para equipos Windows solamente. Ver "Cómo quitar Symantec Management Agent para Windows manualmente" en la página 274.
Use la política de desinstalación de Symantec Management Agent.	La política de desinstalación de Symantec Management Agent se proporciona con Symantec Management Platform. Puede activar dicha política y configurarla para asegurarse de que Symantec Management Agent se ha eliminado de los equipos apropiados. Esta opción está disponible para los equipos con Windows y para UNIX, Linux y Mac. Ver "Cómo configurar las políticas de actualización y de desinstalación de Symantec Management Agent" en la página 268.

Cómo configurar las políticas de actualización y de desinstalación de Symantec Management Agent

Es posible configurar las políticas de actualización de Symantec Management Agent y de desinstalación de Symantec Management Agent para adaptarse a sus requisitos. Ambas políticas utilizan el paquete de Symantec Management Agent, pero utilizan programas distintos.

Ver "Acerca de Symantec Management Agent" en la página 236.

Notification Server ofrece algunos filtros predeterminados que puede utilizar en operaciones de instalación programada del agente y en las políticas de actualización y desinstalación del agente. Estos filtros se almacenan en la carpeta Symantec

Management Agent, en la subcarpeta apropiada. No puede modificar los filtros predeterminados, pero puede duplicarlos para crear filtros nuevos que puede editar para que se adapten a sus requisitos.

Sin embargo, es necesario tener cuidado cuando se realizan las actualizaciones de Symantec Management Agent basadas en los recursos de destino. En entornos de gran magnitud, es probable que prefiera escalonar las actualizaciones, primero utilizando un destino de prueba y luego ejecutando la distribución escalonada a través de destinos apropiados, en lugar de hacerlo todo al mismo tiempo. Por ejemplo, podría haber problemas con la actualización, de modo que puede probarla en una cantidad menor de equipos e identificar y resolver los problemas sin afectar todos los equipos. La actualización escalonada también ayuda a administrar la carga de la red, ya que normalmente los agentes necesitan solicitar datos de Notification Server tan pronto como se actualizan

---

Nota: Mientras realiza la transición de IT Management Suite de versiones anteriores a 7.5, el modo **Comunicación de agente de una versión anterior** (LACA) habilitado permite que un Notification Server actualizado realice un conjunto limitado de funciones de administración en puntos finales con versiones anteriores de Symantec Management Agent. Es posible administrar el modo **Comunicación de agente de una versión anterior** en Symantec Management Console, en la ficha **Procesamiento** de la página **Valores de configuración de Notification Server**.

Ver "Acerca de la comunicación de agente de una versión anterior" en la página 272.

Ver "Cómo configurar los valores de Notification Server" en la página 68.

Para configurar las políticas de actualización y de desinstalación del agente

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Todas las configuraciones**.
2. En el panel izquierdo, expanda **Configuración > Agentes/complementos > Symantec Management Agent** y después realice una de las siguientes acciones:

Para configurar la política de actualización de Symantec Management Agent.	■ Para los equipos de Windows x64, expanda **Windows > Servidor que no es de sitio** y después haga clic en **Symantec Management Agent para Windows x64 (Servidor que no es de sitio) - Actualizar a Symantec Management Agent de 64 bits**. ■ Para los equipos de Windows x86, expanda **Windows > Servidor que no es de sitio** y después haga clic en **Symantec Management Agent para Windows x86 (Servidor que no es de sitio) - Actualizar a Symantec Management Agent de 32 bits**.
Para configurar la política que actualiza Symantec Management Agent en los equipos que contienen uno o más servicios de sitio.	■ Para los equipos de Windows x64, expanda **Windows > Servidor de sitio** y después haga clic en **Symantec Management Agent para Windows x64 (Servidor de sitio solamente) - Actualizar a Symantec Management Agent de 64 bits**. ■ Para los equipos de Windows x86, expanda **Windows > Servidor de sitio** y después haga clic en **Symantec Management Agent para Windows x86 (Servidor de sitio solamente) - Actualizar a Symantec Management Agent de 32 bits**.
Para configurar la política de desinstalación de Symantec Management Agent.	Expanda la carpeta **Windows** y después haga clic en **Symantec Management Agent para Windows: desinstalación**.
Para configurar la política de actualización de Symantec Management Agent para UNIX/Linux/Mac.	Expanda la carpeta **UNIX/Linux/Mac** y después haga clic en **Symantec Management Agent para UNIX/Linux/Mac: actualización**.
Para configurar la política de desinstalación de Symantec Management Agent para UNIX/Linux/Mac.	Expanda la carpeta **UNIX/Linux/Mac** y después haga clic en **Symantec Management Agent para UNIX/Linux/Mac: desinstalación**.

3 En el panel derecho, realice los cambios de configuración apropiados:

Nombre de programa

Nombre del programa del paquete de Symantec Management Agent que se ejecuta cuando se activa la política. La configuración predeterminada establece el programa que es apropiado para la política y no debe cambiarse. No obstante, si ha agregado un programa nuevo al paquete de Symantec Management Agent, quizá desee utilizarlo.

Ver "Cómo administrar programas del paquete" en la página 373.

Habilitar informe detallado de eventos de estado

Habilite el envío de tipos de eventos del estado a Notification Server.

La opción **Captura de evento de Notification Server** de la política **Configuración global de Symantec Management Agent** tiene precedencia sobre la opción **Habilitar informe detallado de eventos de estado** que aparece aquí. Los eventos se envían solamente si están habilitados en la política **Configuración global de Symantec Management Agent**.

Ver "Configuración de las opciones de configuración global de agente" en la página 277.

Se aplica a

Especifique los equipos a los cuales se aplica la política.

Puede utilizar los filtros predefinidos que se proporcionan con Notification Server o crear sus propios filtros.

Ver "Especificación de destinos de una política o tarea" en la página 379.

Multidifusión de paquetes

Deshabilita la descarga de paquetes a través de la multidifusión.

Por lo general, la multidifusión reduce la velocidad de la distribución de los paquetes, de modo que quizá desee desactivarla para instalar revisiones urgentes. Además, en algunos entornos, la multidifusión no funciona. Por ejemplo, es posible que esté deshabilitada en los enrutadores y los conmutadores.

La configuración **Multidifusión de paquetes** de la política **Configuración global de Symantec Management Agent** tiene precedencia sobre la configuración que aparece aquí.

Programación	Especifique la programación de la política. Ver "Cómo especificar una programación de política" en la página 387.

4 Active la política.

En la parte superior derecha de la página, haga clic en el círculo coloreado y, después, en **Activar**.

5 Haga clic en **Guardar cambios**.

Acerca de la comunicación de agente de una versión anterior

El modo **Comunicación de agente de una versión anterior** (LAC) le permite controlar si los equipos que usan las versiones anteriores de Symantec Management Agent se puedan comunicar con la versión actualizada de Notification Server. Esta opción le permite actualizar los agentes en su entorno en fases en lugar de que se actualicen todos inmediatamente después de la actualización de Notification Server.

Según el modo LAC, Notification Server puede administrar los agentes de la siguiente manera:

Se desactiva el modo LAC.	Notification Server puede administrar activamente solo los equipos que tienen la misma versión de Symantec Management Agent que la versión de este Notification Server. Además, Notification Server puede actualizar Symantec Management Agent en los equipos que fueron administrados previamente por el mismo Notification Server.
Se activa el modo LAC.	Notification Server puede realizar un conjunto limitado de las funciones de administración en los equipos que tienen una versión anterior de Symantec Management Agent que la versión de Notification Server. **Nota:** Si se activa el modo LAC, los usuarios que están asociados con el rol **Administradores Symantec** ven un banner de la notificación en la esquina superior derecha de Symantec Management Console, a menos que especifiquen que no se muestre.

Para Symantec Management Agent 7.1 SP1b y versiones posteriores, el modo **Comunicación de agente de una versión anterior** admite la administración de agentes de una versión anterior con los complementos siguientes:

Windows	Software Management, Patch Management, Inventory y pcAnywhere.
UNIX y Linux	Software Management e Inventory.
Mac OS X	Inventory.

Symantec recomienda que desactive el modo LAC después del período de transición de la versión anterior de IT Management Suite a 7.5, para no limitarle a un subconjunto de la funcionalidad que el producto ofrece cuando el modo LAC está activado.

Es posible configurar el modo **Comunicación de agente de una versión anterior** en Symantec Management Console, en la página **Valores de configuración de Notification Server**, en la ficha **Procesamiento**.

Ver "Cómo configurar los valores de Notification Server" en la página 68.

El modo LAC predeterminado en distintas situaciones es de la siguiente manera:

- Si realiza la instalación limpia de IT Management Suite 7.5, se desactiva el modo LAC.
- Si actualiza desde IT Management Suite 7.0 o 7.1 a IT Management Suite 7.5, se activa el modo LAC.
- Si actualiza desde Notification Server 6.x a IT Management Suite 7.5, se activa el modo LAC.

Configuración del paquete de Symantec Management Agent

Las políticas de instalación de Symantec Management Agent usan el paquete apropiado de Symantec Management Agent cuando usted actualiza o desinstala un agente. Le recomendamos que no cambie ninguna configuración en este paquete.

Una vez que se configura un paquete de Symantec Management Agent, es necesario actualizar los puntos de distribución de paquete para actualizar la información del paquete en cada servidor de paquetes.

Ver "Cómo actualizar los puntos de distribución de un paquete" en la página 371.

Para configurar el paquete de Symantec Management Agent

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Todas las configuraciones**.
2. En el panel izquierdo, expanda **Configuración > Agentes/complementos > Symantec Management Agent**.
3. En la carpeta **Windows** o **UNIX/Linux/Mac**, haga clic en el paquete de Symantec Management Agent que desea configurar.
4. En la página **Paquete de Symantec Management Agent**, realice los cambios de configuración necesarios en las fichas apropiadas.

   Para obtener más información, haga clic en la página y después presione **F1**.
5. Haga clic en **Guardar cambios**.

Cómo quitar Symantec Management Agent para Windows manualmente

Es posible quitar manualmente Symantec Management Agent de los equipos que se seleccionan.

Para quitar Symantec Management Agent manualmente

1. En Symantec Management Console, en el menú **Acciones**, haga clic en **Agentes/complementos > Instalar automáticamente Symantec Management Agent**.
2. En la página **Instalación de Symantec Management Agent**, seleccione los equipos Windows de los cuales desea eliminar Symantec Management Agent.
3. En la página **Instalación de Symantec Management Agent**, en **Instalación distribuida del agente en los equipos**, haga clic en **Desinstalar**.

4 En el cuadro de diálogo **Opciones de desinstalación de Altiris Agent**, seleccione las opciones que desee utilizar y especifique la configuración necesaria en los cuadros correspondientes:

Usar proxy (si está configurado en el equipo de destino)	Use esta opción si el equipo que está instalando de forma remota necesita conectarse a Notification Server a través de un servidor proxy. La misma configuración de proxy se usa para conectarse a Notification Server como la configuración de proxy usada por Internet Explorer.
Utilizar la cuenta de administración siguiente	Se necesita una cuenta de administrador para iniciar el servicio de desinstalación en el equipo en el cual se esté eliminando Symantec Management Agent. De forma predeterminada, se usa la identidad de la aplicación Notification Server. Si esta cuenta no tiene permiso para acceder al equipo, debe usarse otra cuenta. Es necesario especificar el nombre de usuario de cuenta de administrador y la contraseña apropiados.

5 Haga clic en **Continuar con la desinstalación**.

Capítulo 17

Cómo configurar Symantec Management Agent

En este capítulo se incluyen los temas siguientes:

- Cómo configurar Symantec Management Agent

Cómo configurar Symantec Management Agent

La configuración predeterminada de Symantec Management Agent es conveniente para un entorno pequeño de Symantec Management Platform. A medida que crece su entorno, o si su organización tiene necesidades especiales, deberá realizar los cambios de configuración apropiados.

Las opciones de configuración del agente se aplican a los equipos administrados apropiados que utilizan las políticas de configuración de agente. Puede modificar estas políticas para cambiar las opciones en cualquier momento. Las nuevas opciones de configuración se aplican a los agentes cuando los equipos administrados reciben sus siguientes actualizaciones de políticas (que generalmente se produce una vez al día).

Tabla 17-1 Tipos de políticas de configuración del agente

Tipo	Descripción
Configuración global	Las opciones de configuración global se aplican a todos los Symantec Management Agents en todos los equipos administrados. Estas opciones de configuración se aplican como una sola política que tienen como destino automático todos los equipos administrados. Ver "Configuración de las opciones de configuración global de agente" en la página 277.

Tipo	Descripción
Configuración de destino	La configuración del agente de destino es el parámetro general que controla a Symantec Management Agent, incluido cómo el agente se comunica con Notification Server. Puede modificar las políticas predeterminadas que se suministran con Symantec Management Platform. Puede crear sus propias políticas de configuración de agente de destino y aplicarlas a los equipos administrados apropiados. Ver "Configuración de las opciones de configuración del agente de destino" en la página 278.
ventanas de mantenimiento	Una ventana de mantenimiento se refiere a una hora y duración programadas en las que se realizan operaciones de mantenimiento en un equipo administrado. Una política de ventana de mantenimiento define una o más ventanas de mantenimiento. Puede modificar la política predeterminada que se suministra con Symantec Management Platform. Puede crear sus propias políticas de mantenimiento de ventana y aplicarlas a los equipos administrados apropiados. Ver "Configuración de políticas de ventana de mantenimiento" en la página 280.

Las políticas de configuración de destino y las políticas de la ventana de mantenimiento se aplican a los equipos administrados que se incluyen en los destinos de política especificados. Estos destinos pueden no ser mutuamente excluyentes. Dos o más políticas del mismo tipo se pueden aplicar al mismo equipo administrado.

Si se aplican dos o más políticas de configuración de destino a un equipo administrado, Notification Server selecciona cuál política utilizar. La selección se basa en el GUID de la política y no es transparente para el usuario. No se puede determinar de antemano qué política se eligió. Sin embargo, una vez realizada la selección, se utiliza de forma consistente para asegurar que se aplique la misma política en todas las actualizaciones.

Si se aplican dos o más políticas de ventana de mantenimiento al mismo equipo administrado, las políticas se fusionarán. Se utilizan todas las ventanas de mantenimiento especificadas.

Configuración de las opciones de configuración global de agente

Las opciones de configuración global son aquellas que no necesitan cambiar de un equipo a otro, por lo tanto se aplican a todos los Symantec Management Agents de todos los equipos administrados. Estas opciones de configuración se aplican

como políticas de configuración global de agente, por lo tanto, se actualizan como cualquier otra política. De forma predeterminada, la política de configuración global de agente se actualiza cada hora. No puede eliminar o desactivar la política de configuración global de agente o crearle versiones alternativas.

Si desea especificar la configuración de agente para grupos específicos de equipos administrados, deberá configurar las políticas de configuración de agente de destino apropiadas.

Para configurar las opciones de configuración global de agente

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Agentes/complementos > Configuración global**.
2. Realice los cambios necesarios en las siguientes fichas:

General	Especifique la configuración de la administración de energía y envío de señales y de la multidifusión de paquetes.
Autenticación	Especifique el nombre de usuario y contraseña que Symantec Management Agent utiliza para conectarse con Notification Server o con un servidor de paquetes.
Eventos	Especifique los eventos de Notification Server que desea capturar.

   Para obtener más información, haga clic en la página y después presione **F1**.

3. Haga clic en **Guardar cambios**.

Ver "Cómo configurar Symantec Management Agent" en la página 276.

Configuración de las opciones de configuración del agente de destino

La política de configuración del agente de destino permite configurar los parámetros generales que controlan Symantec Management Agent, incluida la forma en que el agente se comunica con Notification Server . Es posible aplicar esta configuración a grupos de equipos determinados. Por ejemplo, algunos grupos de equipos pueden tener propósitos diferentes o el usuario puede establecer un tratamiento para los servidores diferente al de los demás equipos administrados. Es posible modificar las directivas predeterminadas que se proporcionan con Notification Server o crear directivas de configuración del agente de destino propias.

Si desea especificar algunas opciones de configuración y aplicarlas a todos los Symantec Management Agents de todos los equipos administrados, es necesario configurar la política de configuración global del agente.

Para configurar los valores del agente de destino

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Agentes/complementos > Configuración del agente de destino**.
2. En el panel izquierdo, realice una de las siguientes acciones:
   - Para crear una nueva política de configuración del agente de destino, haga clic en **Crear nueva**.
   - Para configurar o cambiar el nombre de política, haga clic en la política apropiada y, después, haga clic en **Cambiar nombre**.
     En el cuadro de diálogo **Cambiar nombre del elemento**, escriba el nuevo nombre y haga clic en **Aceptar**.
3. En el panel derecho, realice los ajustes de configuración adecuados en las siguientes fichas:

General	La configuración General incluye la descarga de políticas y las frecuencias de recopilación de inventarios, así como los equipos, los usuarios o los destinos de recursos a los que se aplica la política.
UNIX/Linux/Mac	Si Symantec Management Agent para UNIX, Linux y Mac está instalado, esta ficha se encuentra disponible y proporciona opciones de configuración general para los equipos administrados con UNIX, Linux y Mac.
Descargas	La configuración de descarga controla la forma en que cada agente descarga los paquetes durante las entregas de software. Es posible habilitar las descargas por multidifusión y establecer la multidifusión para las sesiones principales y de clientes. Es posible reemplazar esta configuración por tareas y directivas de entrega de software individuales.
Bloqueos	Los períodos de bloqueo son los momentos en que se deshabilita toda comunicación entre el agente y Notification Server. Es posible establecer cualquier cantidad de períodos de bloqueo.
Control de usuario	Las opciones de configuración de control de usuario son las que afectan lo que el usuario del equipo administrado puede ver.
Opciones avanzadas	Permite especificar una dirección URL alternativa que Symantec Management Agent puede usar para acceder a Notification Server, y activar la función de administración de energía.

Para obtener más información, haga clic en la página y, después, presione **F1**.

4 (Opcional) Para restaurar la política a las opciones de configuración predeterminadas, haga clic en **Restaurar valores predeterminados**.

5 Haga clic en **Guardar cambios**.

Ver "Cómo configurar Symantec Management Agent" en la página 276.

Configuración de políticas de ventana de mantenimiento

Una ventana de mantenimiento se refiere a una hora y duración programadas en las que se realizan operaciones de mantenimiento en un equipo administrado. La operación de mantenimiento cambia el estado del equipo, hace que se reinicie o que interfiera con la capacidad del usuario para operarlo. Por ejemplo, la instalación de parches de sistemas operativos y software o la ejecución de un análisis de virus.

Una ventana de política define una o más ventanas de mantenimiento y se aplica a un destino de recursos de la misma forma que lo haría cualquier otra política. Estas políticas proporcionan la mayor flexibilidad para asignar ventanas de mantenimiento a equipos, sin complicar la administración de las opciones de configuración del agente. Si se aplican varias políticas de ventana de mantenimiento a un solo equipo, se permiten cambios en el equipo durante cualquier ventana de mantenimiento.

Usar las ventanas de mantenimiento le permite programar trabajo de mantenimiento en equipos administrados con un impacto mínimo en el flujo de trabajo y la productividad. También, puede programar el trabajo de mantenimiento en los servidores críticos en momentos diferentes, para que no deban reiniciarse dos servidores simultáneamente. Una ventana de mantenimiento puede programarse para determinados momentos, como todos los días, una vez por semana o una vez por mes. La ventana de mantenimiento puede estar disponible de forma indefinida o puede encontrarse restringida a un intervalo de fechas específico.

Cuando aplica una ventana de mantenimiento a un equipo administrado, las tareas de mantenimiento, como las revisiones o las distribuciones de software, solo pueden realizarse dentro del período de tiempo programado. Los Symantec Management Agents pueden descargar paquetes de distribución de software en cualquier momento, pero los programas asociados pueden ejecutarse solo durante las ventanas de mantenimiento.

Symantec Management Agent procesa la política y proporciona la funcionalidad que utilizan las soluciones para determinar si una ventana de mantenimiento está actualmente abierta. También se proporciona una funcionalidad que permite que las soluciones informen a Notification Server cuando esté en ejecución una tarea de mantenimiento.

Si Symantec Management Agent está ejecutando una tarea como parte de un trabajo cuando caduca una ventana de mantenimiento, la ventana de mantenimiento

se extiende de forma automática hasta que se finalicen todas las tareas que contiene el trabajo.

Puede crear y modificar las políticas de ventana de mantenimiento que necesita y aplicarlas a los destinos apropiados. La política de ventana de mantenimiento predeterminada se aplica a todos los equipos administrados.

Para configurar políticas de ventana de mantenimiento

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Agentes/complementos > Ventanas de mantenimiento**.
2. En el panel izquierdo, realice una de las siguientes acciones:
   - Para crear una nueva política de ventana de mantenimiento, haga clic con el botón derecho en la carpeta **Ventanas de mantenimiento** y después haga clic en **Nueva > Ventana de mantenimiento**.
   - Para modificar una política de ventana de mantenimiento existente, haga clic en la política apropiada.
3. En el panel derecho, en la lista desplegable **Zona horaria**, haga clic en la opción apropiada:

Utilizar la hora del agente	Las horas se especifican sin la información de zona horaria y se aplican a la hora local de cada equipo administrado. Las ventanas de mantenimiento se abren y se cierran en momentos diferentes, dependiendo de la zona horaria de los equipos administrados.
Utilizar la hora del servidor	Las horas se especifican con la información de zona horaria, donde el ajuste de zona horaria corresponde a la zona horaria del servidor donde se ha definido la política. Las ventanas de mantenimiento se abren de forma simultánea sin importar las zonas horarias y se ajustan en horario de verano. Esta opción asegura que las ventanas de mantenimiento se coordinan siempre con la hora local especificada donde se creó la política.
Coordinar mediante UTC	Los horarios se especifican con la información de la zona horaria, donde el ajuste de la zona horaria es 0. Las ventanas de mantenimiento se abren simultáneamente sin importar la zona horaria y no se encuentran afectados por el horario de verano.

La zona horaria se aplica a todas las ventanas de mantenimiento que se especifican en esta política.

4 Si desea que la política se aplique en una fecha determinada, en lugar de tan pronto como se habilite, en la esquina superior derecha, haga clic en **Opciones avanzadas**, después en el cuadro de diálogo **Opciones avanzadas**, establezca las fechas de inicio y finalización, y haga clic en **Aceptar**.

Inicio	La fecha cuando entra en efecto la política. La política debe habilitarse del mismo modo que con cualquier otra política. Es posible habilitar la política en cualquier momento antes o después de la fecha de inicio.
Fin	Si desea que la política esté disponible por un periodo de tiempo limitado, configure la fecha de finalización apropiada. La política no estará disponible luego de dicha fecha, ya sea que esté habilitada o no. Esta configuración es opcional. Si no se especifica una fecha final, la política está disponible de forma indefinida.

5 Para crear las ventanas de mantenimiento que desee incluir en la política, haga clic en **Agregar ventana de mantenimiento**.

6 En cada ventana de mantenimiento, haga lo siguiente:

- En **Horas del día**, especifique la hora de inicio de la ventana de mantenimiento y la hora de finalización o la duración en los cuadros correspondientes.
  Además, puede arrastrar las flechas verde (hora de inicio) y roja (hora de finalización) a los lugares apropiados en la línea de tiempo.
- En **Repetir la programación**, en la lista desplegable **Repetir cada**, seleccione una programación y especifique los filtros de programación adecuados.

7 En **Aplicado a**, especifique el destino de la política de ventana de mantenimiento.

Puede seleccionar un grupo organizativo existente, un filtro o un destino de recursos. También puede seleccionar recursos individuales.

Ver "Especificación de destinos de una política o tarea" en la página 379.

En la cuadrícula se muestran los detalles de los elementos seleccionados. Puede ver la lista por destinos, recursos, equipos o usuarios, y realice las adiciones y eliminaciones necesarias.

8 Haga clic en **Guardar cambios**.

Ver "Cómo configurar Symantec Management Agent" en la página 276.

Sección 5

Implementar la administración habilitada para la nube

- Capítulo 18. Introducir la administración habilitada para la nube
- Capítulo 19. Preparar su entorno para la administración habilitada para la nube
- Capítulo 20. Configurar la administración habilitada para la nube
- Capítulo 21. Realizar las tareas de administración habilitada para la nube

Capítulo 18

Introducir la administración habilitada para la nube

En este capítulo se incluyen los temas siguientes:

- Acerca de la administración habilitada para la nube

Acerca de la administración habilitada para la nube

La administración habilitada para la nube le permite administrar endpoints mediante Internet incluso si los equipos cliente están fuera del entorno corporativo y no pueden acceder a los servidores de administración directamente. Los equipos administrados no necesitan usar una conexión VPN a la red de la organización.

Es posible aplicar administración habilitada para la nube en las situaciones siguientes:

- Una organización con muchos empleados que viajan o que trabajan fuera de la oficina (fuera de la intranet corporativa).
- Un proveedor de servicios administrados (MSP) que administra compañías externas.
- Compañías altamente distribuidas con muchas pequeñas oficinas o empleados que trabajan desde su domicilio.

Cuando se implementa administración habilitada para la nube, no se exponen el equipo con Notification Server ni los servidores de sitio directamente a Internet. Por lo tanto, Symantec Management Agent se comunica con el equipo con Notification Server y los servidores de sitio por medio de un gateway de Internet. Generalmente dos o más gateways de Internet deben estar disponibles para mantener una administración confiable de los clientes habilitados para la nube y para proporcionar opciones de conmutación por error. Cada gateway de Internet puede admitir el enrutamiento a varios Notification Server independientes.

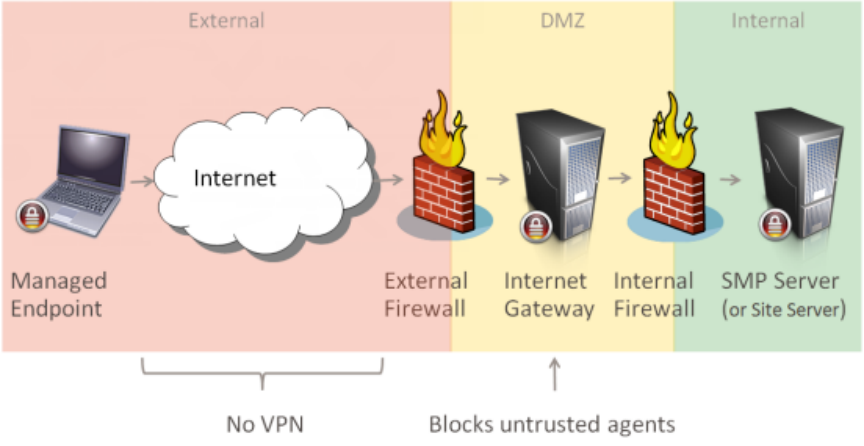
Para usar administración habilitada para la nube, es necesario instalar un servidor del gateway de Internet. El gateway de Internet funciona como proxy de túnel. Asegura la privacidad y la seguridad de los datos que se transfieren entre un agente y un servidor de administración con comunicaciones HTTPS. El gateway de Internet es encuentra en una zona desmilitarizada (DMZ) entre dos firewalls. Acepta conexiones entrantes de equipos cliente autorizados en Internet y las envía a los Notification Server y servidores de sitio apropiados de la red. El gateway de Internet bloquea cualquier intento de conexión por parte de clientes no autorizados.

Symantec Management Agent determina de forma automática si dirigir la comunicación mediante el gateway de Internet es necesario o no. Si un equipo habilitado para la nube tiene acceso directo a la red local usando VPN, el agente cambia de forma automática a una comunicación directa con Notification Server. Si un equipo habilitado para la nube está fuera de la red corporativa, el agente dirige toda la comunicación en Internet a Notification Server mediante el gateway de Internet.

Nota: La administración habilitada para la nube se admite solamente en los equipos cliente con Microsoft Windows.

La administración habilitada en la nube está disponible en su Symantec Management Platform solamente cuando una o más soluciones instaladas admiten administración habilitada en la nube. No todas las soluciones de Symantec admiten administración habilitada para la nube en IT Management Suite 7.5. Para obtener más información sobre el soporte de administración habilitada para la nube para una solución determinada, consulte la documentación de la solución.

Figura 18-1 Administración habilitada para la nube



Para aprovechar la función de administración habilitada para la nube, es necesario realizar las siguientes tareas:

- Configure la infraestructura y configure los servidores y equipos cliente para usar SSL.
  Ver "Preparar su entorno para la administración habilitada para la nube" en la página 287.
- Instale y configure los gateways de Internet, configure las políticas de administración habilitada para la nube y configure los Symantec Management Agent para admitir el entorno de administración habilitada para la nube.
  Ver "Configurar la administración habilitada para la nube" en la página 307.
- (Opcional) Realice tareas de solución de problemas y mantenimiento.
  Ver "Tareas de mantenimiento y solución de problemas habilitadas para la nube" en la página 327.

Capítulo 19

Preparar su entorno para la administración habilitada para la nube

En este capítulo se incluyen los temas siguientes:

- Preparar su entorno para la administración habilitada para la nube

Preparar su entorno para la administración habilitada para la nube

Configurar su entorno para usar SSL es un requisito previo para configurar la administración habilitada para la nube. Una vez que configura su entorno para usar SSL, puede comenzar a configurar la administración habilitada para la nube.

Ver "Configurar la administración habilitada para la nube" en la página 307.

Tabla 19-1 Proceso para preparar su entorno para la administración habilitada para la nube

Paso	Acción	Descripción
Paso 1	Configure su Notification Server y Symantec Management Agent para usar HTTPS.	Primero, debe asegurarse de que sus Notification Server estén configurados para acceso HTTPS y que sus Symantec Management Agent utilicen HTTPS. Notification Server se configura de forma automática para usar HTTPS si selecciona **HTTPS necesario para acceder a la plataforma de administración** en la página **Configuración de Notification Server**, en Symantec Installation Manager, durante la instalación de IT Management Suite. Cuando se inician los Symantec Management Agents desde el Notification Server que usa HTTPS, los Symantec Management Agents también se configuran automáticamente para usar HTTPS. Si instala Notification Server sin soporte de HTTPS, puede configurarlo manualmente más tarde. También debe redirigir los Symantec Management Agents para que usen HTTPS para establecer la comunicación con Notification Server. Ver "Configurar Notification Server para usar HTTPS" en la página 291. Ver "Cómo aplicar un certificado de una autoridad de certificación raíz a un equipo administrado" en la página 292. Ver "Cómo redireccionar Symantec Management Agent para usar HTTPS" en la página 295.

Paso	Acción	Descripción
Paso 2	Prepare los equipos del servidor de sitio.	Se solicita que los equipos cliente habilitados para la nube verifiquen la identidad de los servidores de sitio. Para ese fin, es posible usar un certificado comercial, la propia infraestructura de clave pública (PKI) o Notification Server puede actuar como autoridad de certificación (CA) y generar certificados para los servidores de sitio de Internet. La administración habilitada para la nube no asigna certificados de servidor a los servidores de sitio. Es necesario aplicar certificados de servidor a servidores de sitio para poder acceder a ellos con HTTPS. Un certificado de servidor es un requisito previo para cualquier servidor de sitio que sirva a los Symantec Management Agents en Internet. La herramienta del generador de certificados de servidor de sitio (`AeXGenSiteServerCert.exe`) le permite crear un certificado de servidor de sitio. El nombre del certificado debe coincidir con el nombre del servidor de sitio. Además, este certificado es firmado por el certificado especial de la autoridad de certificación (CA) de Notification Server para los clientes habilitados para la nube. Si no tiene su propia autoridad de certificación de empresa, esta herramienta le permite configurar fácilmente HTTPS en sus servidores de sitio. Para asegurarse de que al agente en el servidor de sitio se pueda comunicar con Notification Server usando HTTPS, también se debe aplicar la autoridad de certificación raíz al equipo servidor de sitio. Ver "Generar y aplicar el certificado de servidor de sitio para el acceso del agente habilitado para la nube" en la página 296. Ver "Cómo aplicar un certificado de una autoridad de certificación raíz a un equipo administrado" en la página 292.
Paso 3	Inicie los servicios de sitio.	Una vez que prepara los equipos servidores de sitio, puede iniciar los servicios de sitio. **Nota:** Ejecutar Task Server en un equipo cliente habilitado para la nube y administrado en Internet no se admite y puede llevar a un comportamiento indeseable. Ver "Administración de servidores de sitio" en la página 131.

Paso	Acción	Descripción
Paso 4	Configure los servidores de paquetes para publicar las bases de código del paquete de HTTPS.	Debe asegurarse de que sus servidores de paquetes o agentes habilitados para la nube puedan recibir paquetes de Notification Server o servidores de paquetes internos. Para permitir que descarguen los paquetes, Notification Server y los servidores de paquetes internos deben publicar las bases de códigos de paquetes de HTTPS. Ver "Configuración de un servidor de paquetes para publicar bases de código de paquetes de HTTPS" en la página 302. Ver "Configuraciones admitidas para los servidores de paquetes en un entorno mixto" en la página 517. **Nota:** Los servidores de paquetes publican bases de códigos con el nombre de dominio completo interno. Si se usa un certificado SSL comercial asignado a Symantec Management Platform, es posible que se produzca un problema de conectividad. Para resolver este problema, consulte el siguiente artículo: TECH210809.
Paso 5	Configure sitios y servidores de sitio para servir a los agentes habilitados para la nube.	Los agentes habilitados para la nube que están detrás del gateway de Internet utilizan sitios de Internet para determinar los servicios de sitio. En Symantec Management Console, es necesario agregar sus servidores de sitio a un **Sitio de Internet predeterminado** o a otros sitios de Internet que desee usar. También debe asignar los equipos habilitados para la nube a los sitios que se basan en los recursos de destino. Esta asignación manual garantiza que cada equipo siga siendo miembro del sitio apropiado, independientemente de dónde esté localizado físicamente. Ver "Configuración de sitios y servidores de sitio para servir a los agentes habilitados para la nube" en la página 304.
Paso 6	Asegúrese de que el sitio de Internet esté configurado correctamente.	En la página del sitio de internet, asegúrese de que los servicios de sitio necesarios estén configurados correctamente y que la configuración se aplique al recurso de destino apropiado. Es posible acceder a la página del sitio de Internet en Symantec Management Console, en la página **Configuración del Servidor de sitio**, en **Administración del sitio > Sitios de Internet**.

Configurar Notification Server para usar HTTPS

Si durante la instalación de IT Management Suite usted no configura su Notification Server para usar HTTPS, debe configurarlo manualmente.

Esta tarea es un paso en el proceso para preparar su entorno para la administración habilitada para la nube.

Ver "Preparar su entorno para la administración habilitada para la nube" en la página 287.

Para configurar Notification Server para usar HTTPS

1. En el equipo con Notification Server, inicie el Administrador de Internet Information Services (IIS).
2. Edite las propiedades del **sitio web de Altiris**.

   Siga el procedimiento que corresponde al sistema operativo del equipo con Notification Server:

Windows 2003	1. En la ventana **Propiedades de Altiris**, en la ficha **Seguridad de directorios**, en **Comunicaciones seguras**, haga clic en **Editar**. 2. En la ventana **Comunicaciones seguras**, seleccione **Requerir canal seguro** y a continuación haga clic en **Aceptar**.
Windows 2008	1. En el panel central, en **IIS**, haga clic en **Configuración de SSL**. 2. Seleccione **Requerir SSL**. 3. En el panel **Acciones**, haga clic en **Aplicar**.

3. Si Notification Server no comienza a publicar las bases de código de HTTPS, haga lo siguiente:
   - Reinicie IIS en Notification Server.
   - Reinicie el servicio de Altiris en Notification Server.
   - En Notification Server ejecute la Programación de actualización del paquete en las tareas programadas de Windows.

Para completar este paso, también es necesario realizar las siguientes acciones:

Ver "Cómo aplicar un certificado de una autoridad de certificación raíz a un equipo administrado" en la página 292.

Ver "Cómo redireccionar Symantec Management Agent para usar HTTPS" en la página 295.

Cómo aplicar un certificado de una autoridad de certificación raíz a un equipo administrado

Antes de migrar un equipo administrado a la administración habilitada para la nube, es necesario asegurarse de que el agente pueda comunicarse con Notification Server y los servidores de sitio que usan HTTPS. Para usar HTTPS para la comunicación, el agente debe confiar en Notification Server y los servidores de sitio. Si es necesario, se pueden agregar los certificados apropiados de la autoridad de certificación (CA) raíz al almacenamiento de **Autoridades de certificados raíz de confianza** de la cuenta de **Equipo Local** en el equipo administrado.

Es posible exportar el certificado autofirmado apropiado de Notification Server. Si Notification Server no usa un certificado autofirmado, deberá exportar la autoridad de certificación raíz para el encadenamiento de certificado que Notification Server usa.

Para aplicar el certificado de CA exportado a un equipo cliente, se puede usar una línea de comandos o Microsoft Management Console. De forma alternativa, se puede usar la política de grupo de Active Directory para iniciar el certificado o para reinstalar Symantec Management Agent con la entrega automática del certificado habilitada.

Esta tarea es un paso en el proceso para preparar su entorno para la administración habilitada para la nube.

Ver "Preparar su entorno para la administración habilitada para la nube" en la página 287.

Para completar este paso, también es necesario realizar las siguientes acciones:

Ver "Configurar Notification Server para usar HTTPS" en la página 291.

Ver "Cómo redireccionar Symantec Management Agent para usar HTTPS" en la página 295.

Para exportar un certificado de CA raíz de Notification Server

1. En el equipo con Notification Server, inicie Microsoft Management Console.
2. Agregue el complemento **Certificados** para **Cuenta de equipo > Equipo local** y después vaya a **Raíz de consola > Certificados (equipo local) > Autoridades de certificación raíz de confianza > Certificados**.

3 Haga clic con el botón derecho en la autoridad de certificación que desee exportar:

SMP <NS_Name> CA de agente	Esta autoridad de certificación emite los certificados del agente. Los Symantec Management Agents usan estos certificados cuando se comunican a través de Notification Server y los servidores de sitio a través de un gateway de Internet. El gateway de Internet debe tener esta autoridad de certificación instalada para confiar en los clientes que se conectan.
SMP <NS_Name> CA de servidor	Esta autoridad de certificación emite los certificados del servidor. Los servidores de sitio usan estos certificados para autenticarse. Cuando los Symantec Management Agents contactan al servidor de sitio, verifican el certificado de servidor.

4 Haga clic en **Todas las tareas > Exportación**.

5 En el Asistente para la exportación del certificado, especifique la configuración siguiente:

- Seleccione **No, no exportar la clave privada**
- Seleccione **DER binario codificado X.509 (.CER)**
- Especifique la ruta y el nombre del archivo de certificado exportado.

6 Haga clic en **Terminar** y, después, cierre la ventana emergente de la confirmación de la exportación.

Es posible después llevar el archivo a un equipo administrado y aplicar el certificado manualmente. Es posible iniciar alternativamente el certificado en los equipos administrados usando una tarea de entrega de paquetes o una política de grupo de Active Directory.

Para aplicar manualmente un certificado de CA raíz a un equipo administrado usando una línea de comandos

1. En el equipo administrado apropiado, ubique el archivo de certificado en la carpeta de instalación de Symantec Management Agent.

   La carpeta predeterminada es la carpeta *C:\\Program Files*\Altiris\Altiris Agent.

2. Abra una ventana de línea de comandos y escriba la siguiente línea de comandos:

   ```
   [carpeta de instalación del agente]\AeXNSAgent.exe
   /rootca=certificateFile.cer
   ```

   Este comando inserta el certificado especificado en el almacén de certificados de las Autoridades de certificación raíz de confianza.

   Por ejemplo:

   C:\\Program Files\Altiris\Altiris Agent\AeXNSAgent.exe /rootca=myClientCert.cer

Para aplicar manualmente un certificado de CA raíz a un equipo administrado usando Microsoft Management Console

1. Ubique el archivo de certificado en una ubicación que sea accesible desde el equipo administrado.
2. En el equipo administrado, inicie Microsoft Management Console.
3. Agregue el complemento **Certificados** para **Cuenta de equipo > Equipo local** y después abra la carpeta **Raíz de consola > Certificados (equipo local)**.
4. Haga clic con el botón derecho en **Autoridades de certificación raíz de confianza** y después seleccione **Todas las tareas > Importación**.
5. En el **Asistente para importar certificado**, especifique la ruta y el nombre del archivo de certificado que desee importar.
6. Haga clic en **Siguiente** para aceptar la ubicación predeterminada y la otra configuración y después haga clic en **Finalizar**.

Para aplicar un certificado de CA de raíz a los equipos administrados reinstalando Symantec Management Agent

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Todas las configuraciones**.
2. En el panel izquierdo, expanda **Agentes/complementos > Symantec Management Agent > Configuración** y, después, haga clic en **Instalación de Symantec Management Agent**.

3 En la página **Instalación de Symantec Management Agent**, en la ficha **Instalar el agente**, en **Instalación distribuida del agente en los equipos**, haga clic en **Configuración**.

4 En el cuadro de diálogo **Opciones de instalación de Symantec Management Agent**, seleccione **Instale el certificado del servidor en el equipo cliente** y haga clic en **Aceptar**.

5 En la página **Instalación de Symantec Management Agent**, en la ficha **Instalar el agente**, en **Instalación distribuida del agente en los equipos**, seleccione los equipos en los cuales instalar Symantec Management Agent y después hacer clic en **Instalar**.

Ver "Tareas de mantenimiento y solución de problemas habilitadas para la nube" en la página 327.

Cómo redireccionar Symantec Management Agent para usar HTTPS

Antes de colocar Symantec Management Agent bajo la administración habilitada para la nube, necesita asegurarse de que el agente use HTTPS para comunicarse con Notification Server. Es posible reorientar el agente para usar HTTPS mediante la política de **Configuración del agente de destino**.

Symantec recomienda crear una política de destino personalizada para los clientes habilitados para la nube y excluir a estos clientes de otras políticas de destino.

Ver "Configuración de las opciones de configuración del agente de destino" en la página 278.

Advertencia: Necesita asegurarse de que el agente confíe en el certificado de servidor SSL que Notification Server usa para las comunicaciones HTTPS. Para aplicar el certificado apropiado a un equipo cliente, se puede usar una línea de comandos o Microsoft Management Console. De forma alternativa, se puede reinstalar Symantec Management Agent con la entrega automática del certificado habilitada.

Ver "Cómo aplicar un certificado de una autoridad de certificación raíz a un equipo administrado" en la página 292.

Esta tarea es un paso en el proceso para preparar su entorno para la administración habilitada para la nube.

Ver "Preparar su entorno para la administración habilitada para la nube" en la página 287.

Para completar este paso, también es necesario realizar las siguientes acciones:

Ver "Configurar Notification Server para usar HTTPS" en la página 291.

Ver "Cómo aplicar un certificado de una autoridad de certificación raíz a un equipo administrado" en la página 292.

Para redireccionar un Symantec Management Agent para usar HTTPS

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Agentes/complementos > Configuración del agente de destino**.
2. En el panel izquierdo, seleccione la política que se aplica a los equipos que desea configurar para la administración habilitada en la nube.
3. En el panel derecho, en la ficha **Opciones avanzadas**, en **URL alternativa para acceder al NS**, seleccione el cuadro.
4. Especifique la URL de HTTPS apropiada que Symantec Management Agent puede usar para acceder a Notification Server:

Nombre del servidor	El nombre del equipo con Notification Server.
Web del servidor	La dirección web de Notification Server. La dirección debe tener el formato siguiente: **https://*NS_FQDN*[:*port*]/Altiris/**

5. Haga clic en **Guardar cambios**.

   Cuando la política se actualiza en el equipo administrado, se redirecciona el agente para usar HTTPS para comunicarse con Notification Server.

El siguiente paso consiste en preparar los equipos de servidor de sitio.

Ver "Generar y aplicar el certificado de servidor de sitio para el acceso del agente habilitado para la nube" en la página 296.

Si desea obtener el proceso completamente detallado de la preparación del entorno para la administración habilitada para la nube, Ver "Preparar su entorno para la administración habilitada para la nube" en la página 287.

Generar y aplicar el certificado de servidor de sitio para el acceso del agente habilitado para la nube

Antes de realizar este paso, asegúrese de haber configurado Notification Server y Symantec Management Agents para que usen HTTPS.

Ver "Configurar Notification Server para usar HTTPS" en la página 291.

Ver "Cómo redireccionar Symantec Management Agent para usar HTTPS" en la página 295.

La administración habilitada para la nube no asigna certificados de servidor a los servidores de sitio. Es necesario aplicar certificados de servidor a servidores de sitio para poder acceder a ellos con HTTPS. Un certificado de servidor es un requisito previo para que cualquier servidor de sitio sirva a los Symantec Management Agents en Internet. Por razones de seguridad, Symantec recomienda usar los certificados autofirmados.

Es necesario usar su propia autoridad de certificación (CA) de empresa para crear los certificados de servidor que se necesitan para configurar HTTPS en los servidores de sitio. Sin embargo, si no tiene su propia autoridad de certificación de empresa, Symantec Management Platform proporciona una herramienta de línea de comandos que permite generar certificados de servidor.

La herramienta del generador de certificados de servidor de sitio, `AeXGenSiteServerCert.exe`, permite crear el certificado de servidor que se necesita. Una autoridad especial de certificación de servidor de Notification Server emite el certificado de servidor. Se almacena la parte pública del certificado en la base de datos de administración de configuración (CMDB). Las partes públicas y privadas se agregan a un archivo PKCS#12 (PFX) que contiene la cadena de certificado completa.

Nota: La herramienta `AeXGenSiteServerCert.exe` solo admite IIS.

Una vez que haya generado el archivo de certificado de servidor, debe instalar el certificado en el servidor de sitio apropiado. El procedimiento de instalación depende de si el certificado de servidor está protegido por contraseña o no. Además depende del sistema operativo del equipo del servidor de sitio.

Tenga en cuenta que los equipos de Task Server deben tener las funciones de IIS 6.0 o IIS 7.0 y de .NET Framework 3.5 habilitadas.

Nota: Aplicar un certificado de servidor regenerado a un gateway de Internet afecta los Symantec Management Agents existentes. Los agentes existentes no pueden conectarse al gateway de Internet hasta que reciben los detalles actualizados de la huella digital de certificado del gateway. Si ningún gateway de Internet alternativo está disponible, es posible que los Symantec Management Agents afectados no puedan conectarse a la red interna. Necesitaría actualizar la configuración del agente manualmente.

Esta tarea es un paso en el proceso para preparar su entorno para la administración habilitada para la nube.

Ver "Preparar su entorno para la administración habilitada para la nube" en la página 287.

Para generar un certificado de servidor para un servidor de sitio

1 En el equipo con Notification Server, abra una ventana de línea de comandos y vaya al siguiente directorio:

```
C:\\Program Files\Altiris\Notification Server\bin\Tools
```

2 Escriba la siguiente línea de comandos con los parámetros apropiados:

```
AeXGenSiteServerCert.exe <SiteServerFQDN> [-o
CertificateChain.pfx] [-p password]
```

SiteServerFQDN	El nombre que Symantec Management Agent usa para conectarse al servidor de sitio. Este nombre es típicamente el nombre de dominio completo (FQDN) del equipo del servidor de sitio. Por ejemplo, su servidor de sitio se puede denominar **mihost.midominio.com**. El nombre en el certificado debe coincidir con el nombre que el agente usa para conectarse al servidor de sitio. Si el nombre o la dirección no coinciden, el agente no puede conectarse al servidor de sitio.
CertificateChain.pfx	El nombre del archivo PFX que desea generar. Si omite este parámetro, el nombre del archivo del certificado generado es el nombre común especificado con la extensión .pfx aplicada a él (***CommonName*.pfx**).
Contraseña	La contraseña que desea usar. Si omite este parámetro, la contraseña está vacía. No se proporciona una contraseña predeterminada. IIS Manager espera que un archivo PFX esté protegido por una contraseña cuando lo importa. Si el archivo PFX no cuenta con ninguna contraseña, primero debe importar el archivo al equipo del servidor de sitio con la Consola de administración de Microsoft (MMC). Es posible entonces usar IIS Manager para aplicar el certificado al elegir asignar un certificado existente.

El archivo de certificado de servidor se crea en el mismo directorio donde se ejecuta el comando.

Para aplicar un certificado de servidor a un servidor de sitio de Windows Vista/7/2008

1. Coloque el archivo PFX de certificado de servidor en el equipo del servidor de sitio o en una ubicación a la que se pueda acceder.
2. En el equipo del servidor de sitio, inicie el Administrador de Internet Information Services (IIS) en el panel izquierdo y haga clic en ***Nombre de equipo***.
3. En el panel medio, haga doble clic en **Certificados de servidor** y a continuación en el panel **Acciones**, haga clic en **Importar**.
4. En el cuadro de diálogo **Importar certificado**, especifique la ruta y el archivo del certificado que desee importar, escriba la contraseña si usted creó el certificado con una contraseña y después haga clic en **Aceptar**.
5. En el Administrador de Internet Information Services (IIS), en el panel izquierdo, en ***Nombre de equipo*** **> Sitios**, haga clic en **Sitio web predeterminado**.
6. En el panel **Acciones**, haga clic en **Vínculos**.
7. En la lista de vínculos, ejecute una de las siguientes acciones:

Cree un nuevo enlace	Haga clic en **Agregar** y configure el tipo **HTTPS**.
Edite un enlace HTTPS existente	Seleccione el enlace y haga clic en **Editar**.

8. En el cuadro de diálogo **Agregar enlace de sitio** o **Modificar enlace de sitio**, especifique el número de puerto para usar, las interfaces de red para escuchar y el certificado SSL que desee usar y después haga clic en **Aceptar**.

   Se espera que el certificado esté en el almacén Personal de la cuenta Equipo local.
9. En el equipo del servidor de sitio, reinicie **IIS** y **Altiris Object Host Services**.

Para aplicar un certificado de servidor protegido por contraseña a un servidor de sitio Windows 2003

1. Coloque el archivo PFX de certificado de servidor en el equipo del servidor de sitio o en una ubicación a la que se pueda acceder.
2. En el equipo del servidor de sitio, inicie el Administrador de IIS y en el panel izquierdo, en ***Nombre de equipo*** **> Sitios web**, haga clic con el botón derecho en **Sitio web predeterminado** y en **Propiedades**.
3. En la ventana **Propiedades de sitio web predeterminado**, en la ficha **Seguridad de directorios**, haga clic en **Certificado de servidor**.
4. En el **Asistente para certificados IIS**, haga lo siguiente:

- En la página **Certificado de servidor**, haga clic en **Importar un certificado desde un archivo .pfx** y haga clic en **Siguiente**.
- En la página **Importar certificado**, especifique la ruta y el nombre de archivo del archivo de certificado y haga clic en **Siguiente**.
- En la página **Contraseña del certificado que desee importar**, escriba la contraseña para el certificado que desee importar.
- En la página **Puerto SSL**, especifique el número de puerto para usar y haga clic en **Siguiente**.
- En la página **Resumen del certificado importado**, verifique los datos del certificado y haga clic en **Siguiente**.
- Haga clic en **Terminar**.

5 Haga clic en **Aceptar** para cerrar la ventana **Propiedades de sitio web predeterminado**.

6 En el equipo del servidor de sitio, reinicie **IIS** y **Altiris Object Host Services**.

Para aplicar un certificado de servidor sin contraseña a un servidor de sitio de Windows 2003

1 En el equipo del servidor de sitio, inicie Microsoft Management Console.

2 Agregue el complemento **Certificados** a la cuenta **Equipo Local** y abra la carpeta **Raíz de consola > Certificados > Personal**.

3 Haga clic con el botón derecho en **Certificados** y en **Todas las tareas > Importar**.

4 En **Asistente para importar certificado**, especifique el archivo de certificado del servidor que desea importar.

5 Haga clic en **Siguiente** para aceptar la configuración predeterminada para todas las páginas restantes en el **Asistente para importar certificado** y haga clic en **Finalizar**.

El certificado se agrega al almacén de certificados Personal.

6 Inicie el Administrador de Internet Information Services (IIS) y, en el panel izquierdo, en ***Nombre de equipo*** **> Sitios web**, haga clic con el botón derecho en **Sitio web predeterminado** y, luego, haga clic en **Propiedades**.

7 En la ventana **Propiedades de sitio web predeterminado**, en la ficha **Seguridad de directorios**, haga clic en **Certificado de servidor**.

8 En el **Asistente para certificados de servidor web**, en la página **Certificado de servidor**, haga clic en **Asignar un certificado ya existente** y, luego, en **Siguiente**.

9 Seleccione el certificado que ha importado y haga clic en **Siguiente** para aceptar la configuración predeterminada para todas las páginas restantes.

10 Haga clic en **Terminar** y, luego, en **Aceptar** para cerrar la ventana **Propiedades de sitio web predeterminado**.

Para aplicar un certificado de servidor a un servidor de sitio de Windows XP

1 Coloque el archivo PFX de certificado de servidor en el equipo del servidor de sitio o en una ubicación a la que se pueda acceder.

2 En el equipo del servidor de sitio, inicie Microsoft Management Console.

3 Agregue el complemento **Certificados** a la cuenta **Equipo Local** y abra la carpeta **Raíz de consola > Certificados > Personal**.

4 Haga clic con el botón derecho en **Certificados** y en **Todas las tareas > Importar**.

5 En el **Asistente para importación de certificados**, especifique el nombre y la ruta del archivo de certificado que desee importar, escriba la contraseña, especifique el almacén de certificados, verifique la configuración y después haga clic en **Terminar**.

6 En el Administrador de IIS, en el panel izquierdo, en ***Nombre de equipo*** **> Sitios web**, haga clic con el botón derecho en **Sitio web predeterminado** y, luego, haga clic en **Propiedades**.

Tenga en cuenta que es necesario tener las funciones de IIS 6.0 o IIS 7.0 y de .NET Framework 3.5 habilitadas.

7 En la ventana **Propiedades de sitio web predeterminado**, en la ficha **Seguridad de directorios**, haga clic en **Certificado de servidor**.

8 En el **Asistente para certificados IIS**, haga lo siguiente:

- En la página **Certificado de servidor**, haga clic en **Asignar un certificado ya existente** y haga clic en **Siguiente**.
- En la página **Certificados disponibles**, haga clic en el archivo de certificado y haga clic en **Siguiente**.
- En la página **Puerto SSL**, especifique el número de puerto para usar y haga clic en **Siguiente**.
- En la página **Resumen del certificado**, verifique los datos del certificado y haga clic en **Siguiente**.
- Haga clic en **Terminar**.

9 Haga clic en **Aceptar** para cerrar la ventana **Propiedades de sitio web predeterminado**.

10 En el equipo del servidor de sitio, reinicie **IIS** y **Altiris Object Host Services**.

Ver "Tareas de mantenimiento y solución de problemas habilitadas para la nube" en la página 327.

El siguiente paso consiste en iniciar los servicios de sitio.

Ver "Administración de servidores de sitio" en la página 131.

Si desea obtener el proceso completamente detallado de la preparación del entorno para la administración habilitada para la nube, Ver "Preparar su entorno para la administración habilitada para la nube" en la página 287.

Configuración de un servidor de paquetes para publicar bases de código de paquetes de HTTPS

Antes de realizar este paso, asegúrese de haber iniciado los servicios de sitio.

Ver "Administración de servidores de sitio" en la página 131.

Es posible configurar HTTPS en los servidores de paquetes en la página **Configuración de Package Service**. Esta página especifica la configuración global del servicio de administración de paquetes que se aplica a todos los servidores de paquetes que sirven a Symantec Management Platform.

El equipo de Package Server debe tener IIS configurado para aceptar las conexiones HTTPS. Es posible usar la autoridad de certificación de empresa interna para proporcionar los certificados apropiados. Si no cuenta con una autoridad de certificación de empresa interna, puede usar una herramienta de línea de comandos de Notification Server para generar los certificados necesarios para la configuración de HTTPS.

Ver "Generar y aplicar el certificado de servidor de sitio para el acceso del agente habilitado para la nube" en la página 296.

Debe asegurarse de que los servidores de paquetes habilitados para la nube puedan servir como origen de descarga para paquetes. Los servidores de paquetes y los agentes habilitados para la nube solamente pueden descargar paquetes usando HTTPS por medio del gateway de Internet. Para permitir a los servidores de paquetes desconectados descargar los paquetes, Notification Server y los servidores de paquetes en el mismo sitio deben publicar las bases de códigos de paquetes de HTTPS. Esta configuración es necesaria porque cuando un servidor de paquetes no tiene ningún origen de paquete disponible dentro de su propio sitio debe solicitarlo de algún otro lugar. El servidor de paquetes, primero, intenta obtener los paquetes de los servidores de paquetes que se encuentran en el mismo sitio

que Notification Server. Si ningún servidor de paquetes está disponible, entonces intenta obtener los paquetes del mismo Notification Server.

Esta tarea es un paso en el proceso para preparar su entorno para la administración habilitada para la nube.

Ver "Preparar su entorno para la administración habilitada para la nube" en la página 287.

Para configurar un servidor de paquetes para publicar bases de código de paquetes de HTTPS

1. Para configurar HTTPS globalmente en todos los servidores de paquetes, haga lo siguiente:
   - En Symantec Management Console, en el menú **Configuración**, haga clic en **Notification Server> Configuración del Servidor de sitio**.
   - En el panel izquierdo, expanda **Administración del sitio > Configuración > Servicio de administración de paquetes** y después haga clic en **Configuración de Package Service**.
   - En la página **Configuración de Package Service**, en **Configuración global de Package Service**, haga clic en **Publicar código base de HTTPS**.
   - Haga clic en **Guardar cambios**.
2. Para configurar un servidor de paquetes individual para usar HTTPS, cree los siguientes valores y claves de registro en cada equipo servidor de paquetes ubicado en el mismo sitio que Notification Server:
   - **Ubicación de registro:** HKEY_LOCAL_MACHINE\SOFTWARE\Altiris\Altiris Agent\Package Server
   - **Tipo de clave:** DWORD
   - **Nombre:** EnableHTTPSOverride
   - **Valor:** 1

   Esta clave de registro anula la configuración de la base de códigos de HTTP en el servidor de paquetes y hace que publique las bases de código de HTTPS en cambio.

El siguiente paso consiste en configurar sitios y servidores de sitio para servir a los agentes habilitados para la nube.

Ver "Configuración de sitios y servidores de sitio para servir a los agentes habilitados para la nube" en la página 304.

Si desea obtener el proceso completamente detallado de la preparación del entorno para la administración habilitada para la nube, Ver "Preparar su entorno para la administración habilitada para la nube" en la página 287.

Configuración de sitios y servidores de sitio para servir a los agentes habilitados para la nube

Antes de realizar este paso, asegúrese de haber configurado los servidores de paquetes para publicar las bases de códigos de HTTPS.

Ver "Configuración de un servidor de paquetes para publicar bases de código de paquetes de HTTPS" en la página 302.

Los equipos que desea administrar por medio de Internet deben organizarse en uno o más sitios. Estos sitios se deben dedicar a agentes habilitados para la nube y no deben contener ningún agente administrado directamente. Se deben entonces asignar los servidores de sitio apropiados a cada sitio.

La administración habilitada para la nube admite Package Servers y Task Servers de Internet, a los que Symantec Management Agent accede a través de un gateway de Internet. La administración habilitada para la nube además admite Package Servers desconectados, que son Package Servers ubicados en el mismo sitio que los agentes habilitados para la nube. Solamente los agentes locales pueden acceder a un Package Server desconectado y usar una conexión directa. Sin embargo, no se admiten Task Servers desconectados.

Los equipos habilitados para la nube deben ser manualmente asignados a los sitios que se basan en los recursos de destino. Los agentes habilitados para la nube no reconocen las asignaciones de sitios basadas en direcciones IP y subredes. La asignación manual asegura que cada equipo siga siendo un miembro del sitio apropiado sin importar dónde el equipo se localiza físicamente.

Ver "Administración de sitios" en la página 129.

Es posible asignar manualmente un agente habilitado para la nube a varios sitios o servidores de sitio. Los servidores de sitio que están disponibles para el agente son una unión de todos los servidores de sitio en los sitios asignados.

Es posible establecer la configuración del servidor de sitio para los agentes habilitados para la nube de las siguientes maneras:

Cree y configure un sitio.	Es posible crear y configurar tantos sitios como sea necesario para adaptarse a la configuración de su entorno. Un agente o un servidor de paquetes habilitado para la nube que es asignado a varios sitios recibe la unión de todos los servidores de sitio en los sitios asignados.

Asigne los agentes habilitados para la nube directamente a los servidores de sitio.	Se puede asignar un recurso de destino directamente al servidor de sitio para asegurarse de otorgar a los miembros de destino el acceso a ese servidor de sitio determinado solamente. El método de asignación por sitio hace que todos los servidores de sitio que son miembros del sitio asignado estén disponibles para los agentes habilitados para la nube de destino.

Nota: Si es necesario, se pueden usar estos dos métodos de asignación juntos.

Esta tarea es un paso en el proceso para preparar su entorno para la administración habilitada para la nube.

Ver "Preparar su entorno para la administración habilitada para la nube" en la página 287.

Para crear y configurar una página de internet para servir los agentes habilitados para la nube

1 En Symantec Management Console, cree un nuevo sitio.

Ver "Administración de sitios" en la página 129.

2 Asigne el recurso de destino apropiado al sitio.

Este recurso de destino contiene los agentes habilitados para la nube y los servidores de paquetes. Es posible reutilizar el mismo recurso de destino que se aplica a la política **Configuración de Administración habilitada para la nube**.

3 Asigne a los servidores de sitio apropiados al sitio en una de las siguientes formas:

Para asignar manualmente el servidor de sitio al sitio	1 En Symantec Management Console, en el menú **Configuración**, haga clic en **Notification Server> Configuración del Servidor de sitio**. 2 En el panel izquierdo, expanda **Administración del sitio > Servidores de sitio > *nombre_de_servidor_de_sitio*** y, luego, haga clic en **Sitios de Internet**. 3 En el panel derecho, en **Información detallada**, haga clic en **Nuevo**. 4 En el cuadro de diálogo **Seleccionar un sitio de Internet**, haga clic en el sitio de Internet al cual desee asignar el servidor de sitio y después haga clic en **Aceptar**.

Para asignar las subredes de los servidores de sitio locales al sitio	1 En Symantec Management Console, en el menú **Configuración**, haga clic en **Notification Server> Configuración del Servidor de sitio**. 2 En el panel izquierdo, haga clic en **Administración del sitio > Subredes**. 3 En el panel derecho, seleccione la subred apropiada. 4 En la barra de herramientas, haga clic en **Asignar a sitio**. 5 En la ventana **Seleccionar un sitio**, seleccione el sitio al cual desee asignar la subred. **Nota:** Un servidor de sitio local es uno que existe en el mismo sitio desconectado que los agentes habilitados para la nube a los que sirve. Este tipo de asignación necesita que el sitio desconectado tenga una subred única que no se superponga con subredes de clientes internos, si hay alguna. Esta configuración no es común, de forma que este enfoque no se recomienda generalmente.

Ver "Cómo asignar un servidor de sitio a un sitio de forma manual" en la página 133.

Para asignar directamente los agentes habilitados para la nube a un servidor de sitio

1 En Symantec Management Console, en el menú **Configuración**, haga clic en **Notification Server> Configuración del Servidor de sitio**.

2 En el panel izquierdo, expanda el servidor de sitio que desee modificar y después haga clic en **Agentes asignados de forma manual**.

3 En el panel derecho, haga clic en **Nuevo**, especifique el recurso de destino que contiene los agentes habilitados para la nube apropiados y después haga clic en **Aceptar**.

Ver "Cómo seleccionar los destinos de recursos con nombre" en la página 386.

El siguiente paso consiste en asegurarse de que el sitio de Internet esté correctamente configurado.

Si desea obtener el proceso completamente detallado de la preparación del entorno para la administración habilitada para la nube, Ver "Preparar su entorno para la administración habilitada para la nube" en la página 287.

Capítulo 20

Configurar la administración habilitada para la nube

En este capítulo se incluyen los temas siguientes:

- Configurar la administración habilitada para la nube

Configurar la administración habilitada para la nube

Antes de que pueda aprovechar la funcionalidad que la administración habilitada para la nube ofrece, es necesario instalar y configurar los gateways de Internet. Después es necesario configurar las políticas de administración habilitada para la nube y además configurar los Symantec Management Agents para admitir el entorno de administración habilitada para la nube.

Antes de que pueda configurar la administración habilitada para la nube, es necesario configurar su entorno para usar SSL.

Ver "Preparar su entorno para la administración habilitada para la nube" en la página 287.

Tabla 20-1 Proceso para configurar la administración habilitada para la nube

Paso	Acción	Descripción
Paso 1	Asegúrese de que la configuración del grupo de aplicaciones sea correcta.	La administración habilitada para la nube requiere que **DefaultAppPool** del equipo con Notification Server use la opción **Integrado** en el **Modo de canalización administrada**. Antes de continuar con la configuración de la administración habilitada para la nube, asegúrese de que se use la opción **Integrado**. Ver "Configuración de DefaultAppPool para usar el modo integrado de canalización administrada" en la página 310.
Paso 2	Establezca la **Configuración del sitio web de IIS para el agente de administración habilitado para la nube**.	Se requiere otro sitio de agente en Notification Server para los agentes habilitados para la nube. Este sitio contiene solamente las interfaces de agente y no proporciona acceso a ninguna de las páginas de Symantec Management Console. También realiza comprobaciones de acceso a recursos y certificados adicionales para aplicar las medidas de seguridad para los agentes que se conectan de Internet. Es necesario configurar el gateway de Internet para permitir el acceso solamente al sitio del agente en Notification Server. Ver "Establecer la configuración del sitio web de IIS para el agente de administración habilitado para la nube" en la página 311.

Paso	Acción	Descripción
Paso 3	Prepare el equipo del gateway de Internet.	El equipo del gateway de Internet debe ubicarse en la zona desmilitarizada (DMZ) de la organización para garantizar que esté protegido tanto en las redes externas como en las internas. Es necesario configurar el firewall en el equipo del gateway para permitir las conexiones entrantes de Internet solamente a los puertos apropiados del gateway. Además es necesario configurar el firewall para permitir conexiones salientes solamente a servidores específicos en su red interna. Si el gateway se ejecuta en una máquina virtual de VMware, es necesario usar el adaptador de red VMXNET 3. Tenga en cuenta que VMXNET 3 está disponible solamente cuando tiene herramientas de VMware instaladas en su máquina virtual. Para obtener más información sobre el adaptador de red VMXNET 3, consulte el artículo de la base de conocimientos siguiente de VMware: KB1001805. El equipo debe tener el sistema operativo Windows Server 2008 R2 SP1 con la función .NET Framework 3.5.1 habilitada. Symantec Management Platform no necesita administrar el equipo de gateway. El gateway de Internet generalmente no es administrado. Antes de iniciar la instalación, es necesario verificar que el equipo de gateway pueda acceder al equipo con Notification Server y a cualquier servidor de sitio necesario. Cuando se verifique la conexión, use los nombres de host, los FQDN o las direcciones IP a los cuales intentan conectarse los agentes habilitados para la nube. Ver "Acerca de la preparación del equipo de gateway de Internet" en la página 313.
Paso 4	Descargue y ejecute el paquete de instalación del gateway de Internet.	Para instalar el gateway de Internet, es necesario descargar y ejecutar el paquete de instalación del gateway de Internet desde Symantec Management Console. Ver "Descarga y ejecución del paquete de instalación del gateway de Internet" en la página 315.

Paso	Acción	Descripción
Paso 5	Configure el gateway de Internet usando el asistente de **Configuración del gateway de Internet de Symantec Management Platform** y el **Administrador del gateway de Internet de Symantec Management Platform**.	En el asistente de **Configuración del gateway de Internet de Symantec Management Platform**, se especifica el puerto para las conexiones entrantes, la información del certificado SSL y la cuenta de usuario. En el **Administrador del gateway de Internet de Symantec Management Platform**, se agrega su Notification Server y sus servidores de sitio a la lista de servidores que puedan comunicarse con el gateway de Internet. Usted además necesita copiar la **Huella digital de certificado del gateway** que se necesita para configurar la política de **Configuración de administración habilitada para la nube**. Ver "Configurar el gateway de Internet" en la página 317.
Paso 6	Configure la política de **Configuración de administración habilitada para la nube**.	La política de **Configuración de administración habilitada para la nube** le permite especificar los equipos que desea administrar por Internet. La política también contiene la lista de gateways de Internet que están disponibles para usar en los equipos cliente de destino. Ver "Configurar la política de Configuración de administración habilitada para la nube " en la página 320. Para colocar los Symantec Management Agents bajo la administración habilitada para la nube, es necesario agregar los equipos apropiados a la política de **Configuración de administración habilitada para la nube**.
Paso 7	Instale Symantec Management Agent en los equipos desconectados.	En algunos casos, es posible que un equipo que desee administrar no tenga acceso a la red que alberga a Symantec Management Platform. Para instalar Symantec Management Agent en un equipo desconectado, es necesario descargar el paquete de instalación del agente de su Symantec Management Console, guardarlo en soportes adecuados y después instalarlo en los equipos apropiados. Ver "Cómo instalar Symantec Management Agent en un equipo desconectado" en la página 323.

Configuración de DefaultAppPool para usar el modo integrado de canalización administrada

La administración habilitada para la nube requiere que **DefaultAppPool** del equipo con Notification Server use la opción **Integrado** en el **Modo de canalización administrada**.

Esta tarea es un paso en el proceso para configurar la administración habilitada para la nube.

Ver "Configurar la administración habilitada para la nube" en la página 307.

Si desea configurar DefaultAppPool para usar el Modo integrado de canalización administrada

1. En el equipo con Notification Server, abra el **Administrador de Internet Information Services (IIS)**.
2. En el **Administrador de Internet Information Services (ISS)**, en el panel **Conexiones**, haga clic en **(Nombre del equipo con Notification Server) > Grupos de aplicaciones**.
3. En el panel **Grupos de aplicaciones**, haga clic en **DefaultAppPool** y, luego, en el panel **Acciones**, haga clic en **Configuración básica**.
4. En la ventana **Modificar grupo de aplicaciones**, en **Modo de canalización administrada**, seleccione **Integrado**. A continuación, haga clic en **Aceptar**.

El siguiente paso consiste en ajustar la **Configuración del sitio web de IIS para el agente de administración habilitado para la nube**.

Ver "Establecer la configuración del sitio web de IIS para el agente de administración habilitado para la nube" en la página 311.

Si desea obtener el proceso completamente detallado de configuración de la administración habilitada para la nube, Ver "Configurar la administración habilitada para la nube" en la página 307.

Establecer la configuración del sitio web de IIS para el agente de administración habilitado para la nube

Antes de realizar este paso, asegúrese de haber configurado **DefaultAppPool** para que use el **modo integrado de canalización administrada**.

Ver "Configuración de DefaultAppPool para usar el modo integrado de canalización administrada" en la página 310.

Se requiere otro sitio de agente en Notification Server para los agentes habilitados para la nube. Este sitio contiene solamente las interfaces de agente y no proporciona acceso a ninguna de las páginas de Symantec Management Console. También realiza comprobaciones de acceso a recursos y certificados adicionales para aplicar las medidas de seguridad para los agentes que se conectan de Internet.

Esta tarea es un paso en el proceso para configurar la administración habilitada para la nube.

Ver "Configurar la administración habilitada para la nube" en la página 307.

Para establecer la configuración del sitio web de IIS para el agente de administración habilitado para la nube

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Notification Server > Administración habilitada para la nube**.
2. En el panel izquierdo, expanda la carpeta **Configuración** y después haga clic en **Configuración del sitio web de IIS para el agente de administración habilitado para la nube**.
3. En la página **Configuración del sitio web de IIS para el agente de administración habilitado para la nube**, seleccione **Agregue el sitio web de IIS para las conexiones con el agente de administración habilitado para la nube** y especifique la siguiente configuración:

Nombre	Permite especificar el nombre con el cual se muestra el sitio web en el **Administrador de Internet Information Services (IIS)**.
Puerto	Permite especificar el puerto en el cual estará disponible el sitio web. Para configurar la administración habilitada para la nube, es necesario que el equipo del gateway de Internet pueda acceder al puerto seleccionado.
FQDN	Permite ver el nombre de dominio completo real del equipo con Notification Server.
Certificado	Permite importar un certificado comercial o crear un certificado SSL autofirmado.

4. Haga clic en **Guardar cambios**.

Nota: La tarea de actualización del paquete es parte del proceso de creación del sitio web. En los entornos en los hay una gran cantidad, esta tarea puede tardar un tiempo considerable. Es posible cerrar Symantec Management Console con seguridad una vez que se registran los siguientes mensajes:

```
Agent site creation task {Task_Guid} started.

Starting Package Refresh for all the packages.
```

El sitio de IIS para el agente de administración habilitado para la nube requiere una conexión que se proteja con un certificado SSL. Es posible importar un certificado comercial o se puede crear un certificado autofirmado. Para usar un certificado comercial, debe cumplir con los siguientes requisitos:

Tabla 20-2 Requisitos de Symantec Management Platform para los certificados SSL

Firma digital	El certificado tiene una firma digital válida.
Confianza	El certificado es emitido por una autoridad de certificación de confianza para el equipo con Notification Server.
Validez	El certificado es válido durante al menos 30 días a partir de la fecha de importación.
Uso de clave mejorado	El valor de Uso de clave mejorado del certificado es el OID de autenticación de servidor (1.3.6.1.5.5.7.3.1).
Nombre del asunto o nombre alternativo del asunto	El nombre del asunto o el nombre alternativo del asunto coincide con el nombre de dominio completo del equipo con Notification Server.
Algoritmo hash	El certificado usa uno de los siguientes algoritmos hash: ■ SHA1 ■ SHA256 ■ SHA384 ■ SHA512
Algoritmo asimétrico	El certificado usa el algoritmo asimétrico RSA.
Formato de archivo	.pfx

El siguiente paso consiste en preparar el equipo del gateway de Internet.

Ver "Acerca de la preparación del equipo de gateway de Internet" en la página 313.

Si desea obtener el proceso completamente detallado de configuración de la administración habilitada para la nube, Ver "Configurar la administración habilitada para la nube" en la página 307.

Acerca de la preparación del equipo de gateway de Internet

Antes de realizar este paso, asegúrese de haber ajustado la configuración del sitio web de IIS para el agente de administración habilitado para la nube.

Ver "Establecer la configuración del sitio web de IIS para el agente de administración habilitado para la nube" en la página 311.

El gateway de Internet de permite a los Symantec Management Agents en Internet comunicarse con Symantec Management Platform. El gateway de Internet reenvía las solicitudes de los Symantec Management Agents autenticados a los números de puerto específicos en las instancias o los servidores de sitio de Notification

Server detrás del gateway. De forma predeterminada, todas las solicitudes se reenvían del puerto HTTPS 443 del gateway al puerto 4726 del equipo con Notification Server.

El gateway de Internet crea un túnel virtual mediante el firewall interno. Permite a clientes autorizados en Internet acceder a los servidores internos apropiados, pero impide el acceso de los clientes no autorizados. Symantec Management Agent habilitado para la nube se comunica con el gateway de Internet directamente por medio de Internet. No se requiere una VPN. Cuando un agente habilitado para la nube se conecta a él, el gateway y el agente intercambian y verifican sus certificados entre sí. El gateway comprueba que un Notification Server conocido haya emitido el certificado de agente. El gateway entonces crea un túnel que el agente puede usar para comunicarse directamente con Notification Server y los servidores de sitio apropiados que usan HTTPS. Cuando el agente finaliza la comunicación con el servidor de destino, finaliza su conexión con el gateway y, a continuación, el gateway destruye el túnel.

La función de administración habilitada para la nube no admite el uso de servidores proxy. No es posible configurar un proxy entre Symantec Management Agent habilitado para la nube y el gateway de Internet.

Symantec recomienda configurar por lo menos dos gateways de Internet para proporcionar opciones de conmutación por error, equilibrio de carga y para mantener la continuidad de comunicación. Cada gateway de Internet puede servir a varios Notification Servers. Se admite esta configuración incluso si los Notification Servers están organizados en una estructura de jerarquía. Cada gateway de Internet admite de 1 a 60 000 endpoints y 3000 conexiones simultáneas.

Los ejemplos siguientes lo ayudan a decidir cuántos gateways de Internet necesita en su entorno:

- Cuando tiene 20 000 clientes en un Notification Server y el 30% de ellos está habilitado para la nube, la práctica recomendada es tener dos gateways de Internet para garantizar la alta disponibilidad. Sin embargo, incluso un gateway de Internet puede manejar fácilmente esta configuración.
- Si tiene 180 000 clientes divididos en dos jerarquías con y el 70% de ellos están habilitados para la nube, usted necesita tener por lo menos cuatro gateways de Internet: tres para manejar la carga del nodo y uno para proporcionar tolerancia de errores.

Antes de instalar el gateway de Internet, es necesario configurar el equipo host. El equipo de gateway debe estar ubicado en la zona desmilitarizada (DMZ) de la organización para asegurarse de que esté protegido de las redes externas e internas. Es necesario configurar el firewall en el equipo del gateway de Internet para permitir las conexiones entrantes de Internet solamente a los puertos

apropiados del gateway. Además es necesario configurar el firewall para permitir conexiones salientes solamente a servidores específicos en su red interna.

Si el gateway se ejecuta en una máquina virtual de VMware, es necesario usar el adaptador de red VMXNET 3. Tenga en cuenta que VMXNET 3 está disponible solamente cuando tiene herramientas de VMware instaladas en su máquina virtual. Para obtener más información sobre el adaptador de red VMXNET 3, consulte el artículo de la base de conocimientos siguiente de VMware: KB1001805.

Nota: El equipo de gateway de Internet debe tener el sistema operativo Windows Server 2008 R2 SP1 con la función .NET Framework 3.5.1 habilitada.

Symantec Management Platform no necesita administrar el equipo de gateway. El gateway de Internet generalmente no es administrado.

Antes de que inicie la instalación, verifique que el equipo de gateway de Internet pueda acceder al equipo con Notification Server y a cualquier servidor de sitio necesario. Cuando verifique la conexión, use los nombres de host o las direcciones IP a los cuales intentan conectarse los agentes habilitados para la nube.

Esta tarea es un paso en el proceso para configurar la administración habilitada para la nube.

Ver "Configurar la administración habilitada para la nube" en la página 307.

Ver "Acerca del equilibrio de carga del gateway de Internet" en la página 521.

El siguiente paso consiste en descargar el paquete de instalación del gateway de Internet.

Ver "Descarga y ejecución del paquete de instalación del gateway de Internet" en la página 315.

Si desea obtener el proceso completamente detallado de configuración de la administración habilitada para la nube, Ver "Configurar la administración habilitada para la nube" en la página 307.

Descarga y ejecución del paquete de instalación del gateway de Internet

Antes de realizar este paso, asegúrese de haber preparado el equipo del gateway de Internet.

Ver "Acerca de la preparación del equipo de gateway de Internet" en la página 313.

Si desea instalar un nuevo gateway de Internet, primero, es necesario obtener el paquete de instalación apropiado del gateway de Internet. El paquete de instalación

es un archivo EXE que se puede descargar de Symantec Management Console. El paquete contiene un instalador que lo guía en el proceso de instalación.

Si puede acceder a Symantec Management Console remotamente desde el equipo de gateway de Internet, puede elegir ejecutar el paquete de instalación del gateway de Internet directamente. De forma alternativa, puede guardar el archivo en cualquier otro soporte, copiarlo en el equipo de gateway de Internet apropiado y después ejecutarlo.

Advertencia: Cierre todos los programas de Windows antes de ejecutar el paquete de instalación del gateway de Internet.

Esta tarea es un paso en el proceso para configurar la administración habilitada para la nube.

Ver "Configurar la administración habilitada para la nube" en la página 307.

Para descargar y ejecutar el paquete de instalación del gateway de Internet

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Notification Server > Administración habilitada para la nube**.
2. En el panel izquierdo, expanda **Configuración** y después haga clic en **Configuración de la Administración habilitada para la nube**.
3. En la página **Configuración de la Administración habilitada para la nube**, en la ficha **Configuración del gateway de Internet**, haga clic en **Descargue el paquete de instalación de gateway de Internet**.
4. Si está en el equipo de gateway, se puede hacer clic en **Ejecutar** para ejecutar el instalador de forma inmediata.

   Si desea guardar el paquete como un archivo para ejecutarlo más tarde o ejecutarlo en otro equipo, haga clic en **Guardar**, especifique la carpeta apropiada y después haga clic en **Aceptar**.
5. Vaya al paquete de instalación del gateway de Internet de SMP que usted descargó y haga doble clic en `SMP_Internet_Gateway`.
6. En el cuadro de diálogo **Abrir archivo: advertencia de seguridad**, haga clic en **Ejecutar**.
7. En el cuadro de diálogo **Configuración de Symantec Management Platform Internet Gateway**, haga clic en **Siguiente**.
8. Haga clic en **Acepto el acuerdo de licencia** y después haga clic en **Siguiente**.

9 Especifique la ruta a la carpeta de destino donde desee instalar los archivos del gateway de Internet, haga clic en **Siguiente** y después haga clic en **Siguiente**.

10 Asegúrese de que el **Iniciar el asistente de configuración** esté seleccionado y después haga clic en **Terminar**.

El siguiente paso consiste en configurar el gateway de Internet.

Ver "Configurar el gateway de Internet" en la página 317.

Si desea obtener el proceso completamente detallado de configuración de la administración habilitada para la nube, Ver "Configurar la administración habilitada para la nube" en la página 307.

Configurar el gateway de Internet

Antes de realizar este paso, asegúrese de haber descargado el equipo de instalación del gateway de Internet.

Ver "Descarga y ejecución del paquete de instalación del gateway de Internet" en la página 315.

Una vez que el gateway de Internet está instalado correctamente, es necesario configurarlo para utilizarlo junto con Symantec Management Platform. Configure el gateway de Internet usando el asistente de **Configuración del gateway de Internet de Symantec Management Platform** y el **Administrador del gateway de Internet de Symantec Management Platform**.

En el asistente de **Configuración del gateway de Internet de Symantec Management Platform**, se especifica el puerto para las conexiones entrantes, la información del certificado SSL y la cuenta de usuario.

En el **Administrador del gateway de Internet de Symantec Management Platform**, se agrega su Notification Server y sus servidores de sitio a la lista de servidores que pueden comunicarse con el gateway de Internet. También obtiene la **Huella digital de certificado del gateway** que se necesita para configurar la política de **Configuración de Administración habilitada para la nube**.

Esta tarea es un paso en el proceso para configurar la administración habilitada para la nube.

Ver "Configurar la administración habilitada para la nube" en la página 307.

Para configurar el gateway de Internet usando el asistente de Configuración del gateway de Internet de Symantec Management Platform

1. En el equipo de gateway de Internet, en el asistente de **Configuración del gateway de Internet de Symantec Management Platform**, en la página **Puertos y direcciones IP**, especifique la dirección IP y los puertos apropiados y después haga clic en **Siguiente**.

   De forma predeterminada, el puerto para las conexiones entrantes es 443. Sin embargo, se puede especificar otro número de puerto si es necesario. Todos los números de puerto especificados deben ser puertos TCP (estos se numeran de 1 a 65 535).

   Debe usar la dirección IP del equipo de gateway de Internet. Es posible especificar solamente un número de puerto y una dirección IP. Si elige usar todas las direcciones IP disponibles, el mismo número de puerto se usa para todas las direcciones IP. Si necesita un control más granular de direcciones IP y de números de puerto, deberá editar el archivo de configuración de Apache directamente.

2. En la página **Información del certificado SSL**, especifique la información apropiada del certificado y después haga clic en **Siguiente**.

   El gateway de Internet debe tener un certificado SSL disponible, de modo que los Symantec Management Agents puedan comunicarse con él. El asistente de configuración genera un certificado SSL autofirmado en función de la información que usted proporciona.

   Si es apropiado, puede usar su propio certificado en vez del certificado autofirmado generado. Es necesario reemplazar manualmente el certificado y los archivos de claves después de la instalación.

   Cree o reciba un certificado y una clave privada de una autoridad de certificación. Almacene el certificado y la clave en los archivos `%installdir%\Apache\certs\server.crt` y `%installdir%\Apache\certs\server.key` respectivamente. El certificado y la clave se deben almacenar en formato PEM no-DES y contienen una cadena de certificación completa. Después reinicie Apache (`httpd.exe`) o use la IU para reiniciar el servicio.

3. En la página **Cuenta de usuario**, especifique la información de cuenta de usuario apropiada y después haga clic en **Siguiente**.

   Por razones de seguridad, debe ejecutar el servicio de gateway de Internet como cuenta de usuario dedicada. Symantec recomienda usar la cuenta **Servicio local**.

4. En la página **Resumen**, revise la configuración y después haga clic en **Terminar**.

Para configurar el gateway de Internet en el Administrador del gateway de Internet de Symantec Management Platform

1. Para abrir el **Administrador del gateway de Internet de Symantec Management Platform**, haga clic en **Inicio > Programas > Administrador del gateway de Internet**.

   Tenga en cuenta que una vez que el asistente de **Configuración del gateway de Internet de Symantec Management Platform** finaliza, el **Administrador del gateway de Internet de Symantec Management Platform** se abre de forma automática.

2. Para agregar sus servidores de sitio y Notification Servers a la lista de servidores que pueden comunicarse con el gateway de Internet, haga lo siguiente:

   - En el **Administrador del gateway de Internet de Symantec Management Platform**, en la ficha **Servidores**, haga clic en **Agregar servidor**.
   - En el cuadro de diálogo **Agregar servidor**, agregue un **Nombre de host** y edite el número de **Puerto SSL** si es necesario. Si agrega un Notification Server, asegúrese de que la opción **Este es un servidor SMP** esté seleccionada. Haga clic en **Aceptar**.

     Tenga en cuenta que el **Puerto SSL** del equipo con Notification Server debe ser igual que el que se especifica en la página **Configuración del sitio de agente de CEM**, en Symantec Management Console.
   - Si aparece el cuadro de diálogo **Advertencia de certificado**, haga clic en **Omitir**.
   - En el cuadro de diálogo **¿Reiniciar servicio?**, haga clic en **Sí**.

3. Para copiar la **Huella digital de certificado del gateway** que se necesita para configurar la política de **Configuración de Administración habilitada para la nube** en Symantec Management Console, haga clic en **Copiar al portapapeles**, en la ficha **General** del **Administrador del gateway de Internet de Symantec Management Platform**.

   Ver "Configurar la política de Configuración de administración habilitada para la nube " en la página 320.

Ver "Scripts de administración del gateway de Internet" en la página 520.

El siguiente paso consiste en configurar la política **Configuración de Administración habilitada para la nube**.

Ver "Configurar la política de Configuración de administración habilitada para la nube " en la página 320.

Si desea obtener el proceso completamente detallado de configuración de la administración habilitada para la nube, Ver "Configurar la administración habilitada para la nube" en la página 307.

Configurar la política de Configuración de administración habilitada para la nube

Antes de realizar este paso, asegúrese de haber configurado el gateway de Internet.

Ver "Configurar el gateway de Internet" en la página 317.

La política de **Configuración de administración habilitada para la nube** le permite especificar los equipos que desea administrar por Internet. La política contiene la lista de gateways de Internet que están disponibles para que usen los equipos cliente especificados. Es posible especificar los gateways de Internet disponibles introduciendo los detalles apropiados de cada gateway.

Usted configuraría normalmente solamente una política de **Configuración de administración habilitada para la nube**. Se necesitan varias políticas solamente si desea tener un control más minucioso sobre qué gateways de Internet sirven qué equipos habilitados para la nube o si desea realizar equilibrio de carga manual

Para generar un paquete de instalación del agente, es necesario crear o seleccionar una política de **Configuración de administración habilitada para la nube** y aplicarla a los equipos de destino apropiados. La lista de gateways de Internet disponibles para la política seleccionada se incluye en el paquete de instalación del agente. Esta lista permite que el agente recién instalado inicie la comunicación con Notification Server de forma inmediata. El nuevo equipo habilitado para la nube se agrega automáticamente al recurso de destino de la política seleccionada.

Cuando Symantec Management Agent recibe la política de **Configuración de administración habilitada para la nube** y no está conectado directamente a Notification Server, intenta conectarse por medio del gateway de Internet. Cuando el agente se conecta correctamente, se convierte en un agente habilitado para la nube. Symantec Management Agent cambia al modo de administración habilitada para la nube solamente cuando se conecta correctamente por medio de un gateway.

Tenga en cuenta que un equipo habilitado para la nube vuelve de forma automática a la comunicación directa con el local Notification Server local cuando un acceso directo a la red está disponible. También vuelve de forma automática al modo habilitado para la nube cuando la conexión directa está ya no disponible. Por ejemplo, un equipo portátil que se usa normalmente en ubicaciones remotas se puede usar de vez en cuando en la oficina conectado a la red interna.

Mientras que la política de **Configuración de administración habilitada para la nube** especifica un equipo, este continúa comunicándose mediante los gateways de Internet apropiados. Si la red interna se configura correctamente, todo el tráfico

entre el agente, el gateway de Internet y Notification Server permanece dentro de la red interna. Sin embargo, si se deshabilita la política de **Configuración de administración habilitada para la nube** o ya no especifica el equipo, el equipo deja de usar el gateway de Internet. El equipo revierte a la comunicación directa con Notification Server local.

Un agente habilitado para la nube mantiene una lista de gateways de Internet que están disponibles para usar. Además, mantiene una lista de servidores de sitio remotos y locales que puede usar. Estas listas se actualizan en el agente cada vez que se actualiza la política de **Configuración de administración habilitada para la nube**.

Esta tarea es un paso en el proceso para configurar la administración habilitada para la nube.

Ver "Configurar la administración habilitada para la nube" en la página 307.

Para configurar la política de Configuración de administración habilitada para la nube

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Notification Server > Administración habilitada para la nube**.
2. En el panel izquierdo, expanda **Política** y después haga clic en **Configuración de Administración habilitada para la nube**.
3. En la página de **Configuración de Administración habilitada para la nube**, configure la política de la siguiente manera:

Configure la lista de gateways de Internet que aceptan tráfico de agentes externos.	Para agregar un gateway de Internet, en el cuadro de diálogo **Editar servidor de puerta de enlace**, especifique sus parámetros de la siguiente manera: ■ **Servidor** El nombre de dominio completo (FQDN) del equipo de gateway de Internet. ■ **Puerto** El número de puerto que Symantec Management Agent debe usar para conectarse al gateway de Internet. El puerto predeterminado es el 443. ■ **Huella digital** Pegue el valor de la **Huella digital de certificado del gateway** que copió en el equipo de gateway de Internet, en el **Administrador del gateway de Internet de Symantec Management Platform**, en la ficha **General**. Ver "Configurar el gateway de Internet" en la página 317.

Especifique los equipos de destino a los cuales se aplica la política.	Si desea habilitar la administración habilitada para la nube en los Symantec Management Agent, es necesario agregar estos equipos a la política. Una vez que el agente en un equipo cliente recibe la política de **Configuración de administración habilitada para la nube**, se conecta a Notification Server y solicita su certificado de cliente único. Cuando el agente ha recibido su certificado y no tiene ninguna conexión directa a Notification Server, intenta conectarse mediante los gateways de Internet disponibles que se especificaron en la política. Una vez que el agente se conecta correctamente, cambia del modo administrado directamente y se convierte en agente habilitado para la nube. **Advertencia:** Si planea usar el paquete de instalación para instalar agentes en equipos desconectados, es necesario incluir esos clientes en la política. Si no lo hace, se elimina la configuración del gateway para estos clientes cuando se conectan directamente a la red local. Se elimina la configuración del gateway para los clientes porque no son miembros automáticos de la política de **Configuración de administración habilitada para la nube**. Por lo tanto, debe definir el ámbito de los clientes antes de iniciar el paquete de instalación. Ver "Especificación de destinos de una política o tarea" en la página 379.

4 Active la política.

En la parte superior derecha de la página, haga clic en el círculo coloreado y, después, en **Activado**.

5 Haga clic en **Guardar cambios**.

Una vez que Symantec Management Agent recibe la política, está listo para utilizar la función de administración habilitada para la nube. Hasta que el equipo cliente se conecta a la red interna, el modo de administración habilitada para la nube permanece deshabilitado. Cuando se desconecta el equipo cliente de la red interna y Symantec Management Agent puede conectarse a Notification Server por medio de un gateway de Internet, la administración habilitada para la nube se activa de forma automática

Es posible comprobar el estado del modo de administración habilitada para la nube en Symantec Management Agent del equipo cliente, en la ficha **Configuración de Symantec Management Agent**, en **Estatus de la red**.

El siguiente paso consiste en instalar Symantec Management Agent en un equipo desconectado.

Ver "Cómo instalar Symantec Management Agent en un equipo desconectado" en la página 323.

Si desea obtener el proceso completamente detallado de configuración de la administración habilitada para la nube, Ver "Configurar la administración habilitada para la nube" en la página 307.

Cómo instalar Symantec Management Agent en un equipo desconectado

Antes de realizar este paso, asegúrese de haber configurado la política de configuración de la administración habilitada para la nube.

Ver "Configurar la política de Configuración de administración habilitada para la nube " en la página 320.

En algunos casos, es posible que un equipo que desee administrar no tenga acceso a la red que alberga a Symantec Management Platform. Para instalar Symantec Management Agent en un equipo desconectado, primero necesita descargar el paquete de instalación del agente de Symantec Management Console.

Ver "Parámetros del paquete de instalación del agente habilitado para la nube" en la página 522.

Una vez que genera el paquete de instalación del agente de la instancia apropiada de Symantec Management Platform, debe enviar el agente al sitio remoto desconectado. Es posible enviar el paquete por correo electrónico o enviarlo en un medio físico, como CD o unidad flash. Los usuarios en el sitio remoto ejecutan el paquete de instalación del agente para instalar Symantec Management Agent en sus equipos. El Symantec Management Agent recientemente instalado se conecta de forma inmediata a Notification Server mediante el gateway de Internet apropiado. Es posible usar el mismo paquete de instalación para instalar Symantec Management Agent en todos los equipos en un sitio remoto determinado. Sin embargo, todos los agentes recién instalados comparten la misma configuración, de manera que se deben usar los mismos gateways de Internet y conectar al mismo Notification Server.

Nota: Si desea usar el paquete de instalación para instalar agentes en un equipo desconectado, es necesario crear una política que incluya esos clientes. Si no lo hace, se elimina la configuración del gateway para estos clientes cuando se conectan directamente a la red local. Se elimina la configuración del gateway para los clientes porque no son miembros de la política de **Configuración de administración habilitada para la nube**. Por lo tanto, debe definir el ámbito de los clientes antes de iniciar el paquete de instalación.

Esta tarea es un paso en el proceso para configurar la administración habilitada para la nube.

Ver "Configurar la administración habilitada para la nube" en la página 307.

Para instalar Symantec Management Agent en un equipo desconectado

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Notification Server > Administración habilitada para la nube**.
2. En el panel izquierdo, expanda **Configuración** y después haga clic en **Configuración de la Administración habilitada para la nube**.
3. En la página **Configuración de la Administración habilitada para la nube**, en la ficha **Configuración de Symantec Management Agent**, haga clic en **Generar y descargar paquete de instalación de Symantec Management Agent**.
4. En el cuadro de diálogo **Paquete de instalación de agente habilitado para la nube**, especifique los parámetros apropiados del paquete.

   Para obtener más información, haga clic en la página y después presione **F1**.

   Ver Tabla C-5 en la página 522.
5. Haga clic en **Generar paquete de instalación del agente**.

   La generación del paquete puede tardar varios minutos. Cuando el paquete esté listo, se le solicitará ejecutar o guardar el archivo.

   El paquete de instalación generado es un paquete de instalación autoextraíble del agente que incluye los componentes y la configuración siguientes:

   - Instalador de Symantec Management Agent para la plataforma apropiada.
   - Dirección de Notification Server (incluido el protocolo y el número de puerto que se usará).
   - Certificado de Notification Server con cadena de CA.
     El gateway de Internet certifica la huella digital y el certificado de sitio. El certificado de sitio se usa para conectarse al gateway por primera vez. El certificado de sitio es esencial, ya que se usa para generar una solicitud de certificado de cliente permanente.

- Lista de los gateways de Internet que están disponibles para que los use el agente habilitado para la nube.
- Recurso de destino al cual el equipo se agrega automáticamente.
- Grupo organizativo al cual el equipo se agrega automáticamente.
- Scripts para configurar Symantec Management Agent para usar la configuración especificada.

Advertencia: El paquete de instalación de Symantec Management Agent es válido por un tiempo limitado (de forma predeterminada, siete días) a partir de la fecha en que se genera. El certificado de sitio temporal que se incluye en el paquete caduca después de esta fecha. Si usa el paquete después de la fecha de caducidad del certificado de sitio, el agente instalado no puede usar el gateway de Internet para comunicaciones. Es necesario reinstalar el agente con un paquete de instalación recientemente generado que contenga un certificado de sitio válido.

---

6 En el cuadro de diálogo **Descarga de archivos**, haga clic en **Guardar** y especifique la ubicación en la cual desea guardar el archivo.

7 Cuando la descarga del paquete se complete, haga clic en **Cerrar**.

8 En el cuadro de diálogo **Paquete de instalación de agente habilitado para la nube**, haga clic en **Cerrar**.

9 Coloque el paquete de instalación de Symantec Management Agent en el equipo desconectado apropiado.

10 Ejecute el paquete de instalación del agente en el equipo desconectado.

El paquete del agente es un archivo ejecutable autoextraíble y la instalación se ejecuta de forma silenciosa.

Después de la instalación, Symantec Management Agent de forma automática se configura y hace lo siguiente:

- El agente renegocia su certificado.
  El agente solicita y recibe un nuevo certificado de Notification Server: El nuevo certificado es específico de ese equipo cliente y reemplaza el certificado de sitio temporal que fue incluido en el paquete de instalación del agente.

- El agente se asigna automáticamente a los recursos de destino y a los grupos organizativos apropiados en Symantec Management Platform.

11 Verifique que la instalación se haya ejecutado correctamente. Es posible usar Symantec Management Console para ver los informes y comprobar que el equipo administrado recientemente está presente.

Si especificó un grupo organizativo en el paquete de instalación, puede también comprobar que el nuevo equipo se haya agregado al grupo apropiado.

Ver "Visualización de informes de administración habilitada para la nube" en la página 338.

Si desea obtener el proceso completamente detallado de configuración de la administración habilitada para la nube, Ver "Configurar la administración habilitada para la nube" en la página 307.

Capítulo 21

Realizar las tareas de administración habilitada para la nube

En este capítulo se incluyen los temas siguientes:

- Tareas de mantenimiento y solución de problemas habilitadas para la nube

Tareas de mantenimiento y solución de problemas habilitadas para la nube

Esta sección resume las tareas de mantenimiento y solución de problemas que puede necesitar realizar.

Ver "Acerca de la administración habilitada para la nube" en la página 284.

Tabla 21-1 Tareas de mantenimiento y solución de problemas habilitadas para la nube

Tarea	Descripción
Cómo aplicar una autoridad de certificación raíz a un equipo administrado.	Antes de que pueda migrar un equipo administrado directamente a la administración habilitada para la nube, debe asegurarse de que el agente pueda comunicarse con Notification Server usando el HTTPS. El agente debe confiar en Notification Server para usar HTTPS para la comunicación. Si es necesario, se puede agregar una autoridad de certificación raíz (CA) al almacén **Autoridades de certificación raíz de confianza** en el equipo administrado. Ver "Cómo aplicar un certificado de una autoridad de certificación raíz a un equipo administrado" en la página 292.

Tarea	Descripción
Cómo generar un certificado de cliente temporal.	La administración habilitada para la nube asigna certificados de cliente a equipos administrados y servidores de sitio, de modo que puedan identificarse en Notification Server. Es posible que sea necesario generar un certificado de cliente temporal para un equipo administrado. Una herramienta del generador de certificado de cliente (`AeXGenClientCert.exe`) está disponible en Notification Server. Ver "Cómo generar un certificado de cliente temporal" en la página 328.
Cómo instalar un certificado de cliente temporal en un equipo administrado.	Si Symantec Management Agent deja de comunicarse a través de los gateways de Internet, su certificado se puede dañar. Es posible restaurar la comunicación instalando un certificado de cliente temporal en el equipo administrado apropiado. Symantec Management Agent usa el certificado temporal para reparar la conectividad con el gateway de Internet. Es posible agregar o eliminar certificados del almacén de certificados del servicio de agente según sea necesario. Ver "Cómo instalar un certificado temporal en un equipo administrado" en la página 331.
Cómo revocar un certificado de cliente en un equipo administrado.	Si cree que el certificado de un cliente determinado está en peligro y ya no debe confiar en él, se puede revocar el certificado. Por ejemplo, si se pierde o se roba un equipo portátil habilitado para la nube, es necesario revocar el certificado de forma inmediata. Revocar el certificado evita que el equipo administrado acceda a su red en el modo habilitado para la nube. Ver "Revocar un certificado de administración habilitada para la nube" en la página 332.
Forzar un agente habilitado para la nube a usar un gateway de Internet especificado.	Si el agente no tiene una lista válida de gateways de Internet, se puede forzar para que se comunique mediante un conjunto especificado de gateways. Es posible agregar y eliminar gateways de Internet de la lista según sea necesario. Ver "Cómo forzar Symantec Management Agent para usar un gateway de Internet especificado" en la página 335.
Copia de seguridad y restauración del gateway de Internet.	Es posible hacer una copia de seguridad de la configuración del gateway de Internet y restaurar su estado original en caso de que se produzca un error. Ver "Hacer copia de seguridad de un gateway de Internet y restaurarlo" en la página 336.
Visualización de informes de administración habilitada para la nube.	Se proporciona un conjunto de informes predefinidos para ayudarlo a supervisar y administrar sus equipos habilitados para la nube. Ver "Visualización de informes de administración habilitada para la nube" en la página 338.

Cómo generar un certificado de cliente temporal

La administración habilitada para la nube asigna certificados de cliente a equipos administrados y servidores de sitio, de modo que puedan identificarse en Notification

Server. La herramienta del generador de certificado de cliente (`AeXGenClientCert.exe`) le permite crear los certificados de cliente que necesita. El certificado de la autoridad de certificación (CA) de Notification Server Agent emite estos certificados. Se almacena la parte pública del certificado en la base de datos de administración de configuración (CMDB). Las públicas y privadas se agregan a un archivo PKCS#12 (PFX).

Nota: El certificado generado es válido por un período limitado. De forma predeterminada, este período es de siete días, pero se puede cambiar si es necesario.

Es posible que sea necesario generar un certificado temporal para un equipo administrado. Es necesario generar el archivo PFX apropiado e instalar el archivo en el equipo administrado o el servidor de sitio.

Para generar un certificado de cliente

- En el equipo con Notification Server, abra una ventana de línea de comandos y ejecute la siguiente línea de comandos con los parámetros apropiados:

  ```
  \Program Files\Altiris\Notification
  Server\bin\Tools\AeXGenClientCert <CommonName> [-o
  Certificate.pfx] [-p password]
  ```

CommonName	El identificador que desea mostrar en la línea de asunto del certificado. Este identificador se usa para informar y diagnosticar propósitos. Este identificador debe ser igual al parámetro **Nombre de instalación** que se especificó en el paquete de instalación de Symantec Management Agent. Ver "Parámetros del paquete de instalación del agente habilitado para la nube" en la página 522.
Certificate.pfx	La ruta completa y el nombre del archivo PFX que desea generar. Si omite este parámetro, el certificado generado se guarda en el directorio local. Al archivo de certificado se le otorga un nombre después de que el nombre común especificado con la extensión .pfx se aplica a él (***CommonName*.pfx**).
Contraseña	La contraseña que desea usar. Si omite este parámetro, la contraseña está vacía. No se aplica una contraseña predeterminada.

  El nombre y la ruta al archivo generado se muestran en la ventana de línea de comandos.

  Copie el archivo de certificado generado en los soportes correspondientes y colóquelo en la carpeta raíz del equipo cliente apropiado. A continuación, en el equipo cliente, use el conmutador de línea de comandos `/importcert` para lograr que Symantec Management Agent use el certificado.

  Ver "Cómo instalar un certificado temporal en un equipo administrado" en la página 331.

Ver "Tareas de mantenimiento y solución de problemas habilitadas para la nube" en la página 327.

Cómo instalar un certificado temporal en un equipo administrado

Si Symantec Management Agent deja de comunicarse a través de los gateways de Internet, su certificado se puede dañar. Es posible resolver este problema instalando un certificado temporal en el equipo cliente apropiado.

Symantec Management Agent usa el certificado temporal para conectarse a Notification Server a través del gateway de Internet apropiado. A continuación, solicita un nuevo certificado único a ese equipo.

El archivo de certificado debe incluir una clave privada y no tener ninguna contraseña asociada.

Para instalar un certificado temporal en un equipo administrado

1. Genere un certificado de cliente temporal, *tempcert.pfx*.

   Es posible usar una herramienta de la línea de comandos en el equipo con Notification Server para generar un certificado de cliente temporal. La herramienta de la línea de comandos genera un archivo PFX que contiene el certificado y la clave privada.

   Ver "Herramientas de la línea de comandos de Notification Server" en la página 516.

   Nota: De forma predeterminada, el archivo generado no tiene contraseña. No especifique una contraseña, pues Symantec Management Agent no puede usar los archivos protegidos por contraseña de PFX.

   Ver "Cómo generar un certificado de cliente temporal" en la página 328.

2. Ponga el archivo PFX generado en la carpeta raíz del equipo administrado.

3. Abra una ventana de línea de comandos y ejecute la línea de comandos siguiente:

   ```
   [carpeta de instalación del agente]\AeXNSAgent.exe
   /importcert=tempcert.pfx
   ```

   Por ejemplo:

   \Program Files\Altiris\Altiris Agent\AeXNSAgent.exe /importcert=myRootCert.pfx

4. Reinicie Symantec Management Agent para hacer que la nueva configuración surta efecto.

Para eliminar un certificado de un equipo administrado

- En el equipo administrado, abra una ventana de línea de comandos y ejecute la línea de comandos siguiente:

  ```
  [carpeta de instalación del agente]\AeXNSAgent.exe /removecert
  ```

  Este comando quita el certificado actual de Symantec Management Agent.

  Por ejemplo:

  \Archivos de programa\Altiris\Altiris Agent\AeXNSAgent.exe /removecert

Ver "Tareas de mantenimiento y solución de problemas habilitadas para la nube" en la página 327.

Ver "Conmutadores de línea de comandos para la configuración de agentes habilitados para la nube" en la página 523.

Revocar un certificado de administración habilitada para la nube

Revocar un certificado de administración habilitada para la nube (CEM) evita que el equipo administrado acceda a su red en el modo habilitado para la nube. Por ejemplo, si se pierde o se roba un equipo portátil habilitado para la nube, es necesario revocar el certificado de forma inmediata.

El agente tiene dos certificados de CEM. Un certificado permite al agente crear la conexión al gateway de Internet y otro certificado permite al agente conectarse a Notification Server. Si se revoca el certificado que permite al agente conectarse a Notification Server, Notification Server declina la conexión de ese cliente. Sin embargo, el gateway de Internet no tiene ninguna capacidad de recibir información sobre los certificados revocados de Notification Server directamente. Para revocar un certificado determinado en el gateway de Internet, es necesario agregar los detalles del certificado a la Lista de revocación de certificados (CRL) en Notification Server, generar un archivo de CRL actualizado y después aplicar el archivo CRL actualizado al gateway de Internet apropiado.

Nota: Es necesario aplicar el archivo CRL actualizado a cada gateway de Internet que el agente revocado pueda usar.

Tenga en cuenta que la revocación del certificado habilitado para la nube solo bloquea el acceso del equipo administrado a Notification Server en el modo habilitado para la nube. Si la confianza del agente no se revoca, el agente puede continuar funcionando en el modo local.

Para revocar un certificado de administración habilitada para la nube

1. En Symantec Management Console, en el menú **Informes**, haga clic en **Todos los informes**.
2. En el panel izquierdo, en **Informes**, expanda **Administración de Notification Server > Certificados** y después haga clic en **Certificado por huella digital**.
3. En la página del informe **Certificado por huella digital**, haga clic con el botón derecho en el certificado que desea revocar y después haga clic en **Revocar certificado**.

   Si revoca el certificado en la página del informe **Certificado por huella digital**, los detalles del certificado se agregan al archivo CRL de forma automática.

   El CRL se almacena en el almacén del equipo raíz, aunque los certificados se almacenen en la base de datos de administración de configuración (CMDB). La herramienta de revocación de certificado, (`AeXRevokeCertificate.exe`) primero carga el CRL existente, si existe uno. Si no existe ninguna CRL en el almacén de certificados, la herramienta crea una. La herramienta después agrega el número de serie del certificado a la lista y genera un archivo con codificación PEM que contiene la CRL actualizada. Después coloca el archivo de CRL generado en el equipo de gateway de Internet y ejecuta un script para aplicar la lista actualizada al gateway de Internet.

   De forma predeterminada, el archivo CRL está en la siguiente ubicación en Notification Server:

   ```
   \Program Files\Altiris\Notification
   Server\bin\Tools\AeXRevokeCertificate\EMEncodedFile.CRL
   ```

Para agregar un certificado de administración habilitada para la nube al CRL manualmente

1. Obtenga el número de serie y la huella digital del certificado de cliente que desea revocar.

   Si tiene acceso al equipo cliente, se puede usar Microsoft Management Console (MMC) para buscar los detalles del certificado de cliente.

   Si no tiene acceso al equipo cliente, puede usar algunos de los siguientes métodos:

   - En Symantec Management Console, abra el Administrador de recursos y consulte la información del inventario básico para el equipo cliente. La ruta del menú es **Ver > Clases de datos > Inventario > Inventario básico > Certificado de AeX AC**. Se muestran los detalles completos del certificado de cliente, incluidos el número de serie y la huella digital.

- Realice búsquedas en la CMDB de Symantec Management Platform con una consulta de SQL. Los certificados de cliente se almacenan en la tabla **Registro de certificado**.
- En el gateway de Internet, abra el archivo de registro del acceso y busque una entrada que se relacione con el cliente. El archivo access.log se almacena en la carpeta Apache\logs en la carpeta de instalación del gateway de Internet. Cada entrada en el archivo de registro incluye el nombre del equipo que accedió al gateway de Internet y el número de serie del certificado correspondiente.

2 En el equipo con Notification Server, abra una ventana de línea de comandos y ejecute la siguiente línea de comandos con los parámetros apropiados:

```
\Archivos de programa\Altiris\Notification
Server\bin\Tools\AeXRevokeCertificate -o <PEMEncodedFile.CRL> <-t
Sha1ThumbPrint | -s SerialNumber>
```

PEMEncodedFile.CRL	La ruta completa y el nombre del archivo de CRL con codificación PEM que desee generar. Si omite este parámetro, el archivo generado se guarda en el directorio local.
Sha1ThumbPrint	El identificador único del certificado.
Número de serie	Si más de un certificado en la base de datos tiene el mismo número de serie, use una huella digital SHA-1 para identificar el certificado. Por el contrario, si dos certificados tienen la misma huella digital, identifique el certificado por número de serie. **Nota:** En algunos lugares, la huella digital y el número de serie se pueden mostrar como octetos separados por espacios. Sin embargo, cuando se especifican como parámetros de línea de comandos, no deben incluir caracteres de espacio.

Se genera el archivo CRL actualizado.

Para aplicar el CRL a un gateway de Internet

1. Coloque el CRL generado en la siguiente ubicación en el equipo de gateway de Internet:

   `[carpeta de instalación del gateway de Internet]\Apache\certs\crl`

   La carpeta de instalación predeterminada del gateway de Internet es `\Program Files x86\Symantec\SMP Internet Gateway`. Sin embargo, la ruta depende del directorio de destino que fue especificado durante la instalación del gateway de Internet.

2. En la misma carpeta, haga doble clic en **UpdateCrlHashes.cmd** para ejecutar el script **Actualización de CRL**.

   Este script realiza la configuración necesaria y después reinicia el gateway de Internet para que los cambios surtan efecto.

Ver "Tareas de mantenimiento y solución de problemas habilitadas para la nube" en la página 327.

Cómo forzar Symantec Management Agent para usar un gateway de Internet especificado

Si el agente no tiene una lista válida de gateways de Internet, se puede forzar para que se comunique mediante un conjunto especificado de gateways. Se fuerza una lista específica de gateways desde la línea de comandos o modificando la configuración del registro. Una línea de comandos está disponible para agregar los gateways individuales.

Si desea eliminar un gateway de Internet de la configuración de Symantec Management Agent, puede hacerlo editando el registro.

Los detalles del gateway de Internet se almacenan en el registro. Es posible agregar o eliminar los gateways de Internet editando las entradas conforme a la clave siguiente:

`HKEY_LOCAL_MACHINE\SOFTWARE\Altiris\Communications\Secure Gateways`

Cada gateway de Internet tiene un conjunto de valores conforme a la clave `<GatewayName>`.

Nota: Es necesario reiniciar Symantec Management Agent para que esta configuración surta efecto.

Para forzar Symantec Management Agent para usar un gateway de Internet especificado

- En el equipo cliente, abra una ventana de línea de comandos y ejecute la línea de comandos siguiente:

```
\Archivos de programa\Altiris\Altiris Agent\AeXNSAgent.exe
/gw=gatewayName,port,thumbprint
```

gatewayName	El nombre o la dirección IP del equipo de gateway.
puerto	El número de puerto que Symantec Management Agent debe usar para conectarse al gateway. El puerto predeterminado es 443.
Huella digital	La huella digital de certificado que el gateway usa para las conexiones seguras. **Nota:** En algunos lugares, la huella digital se puede mostrar como octetos separados por espacios. Sin embargo, cuando se especifica como un parámetro de línea de comandos, no debe incluir ningún carácter de espacio.

Cada parámetro debe ser separado con una coma. No se permiten espacios ni otra puntuación.

Por ejemplo:

\Program Files\Altiris\Altiris Agent\AeXNSAgent.exe /gw=myGateWay.symantec.com,443,0f8753ef3da6bc4

Ver "Tareas de mantenimiento y solución de problemas habilitadas para la nube" en la página 327.

Ver "Conmutadores de línea de comandos para la configuración de agentes habilitados para la nube" en la página 523.

Hacer copia de seguridad de un gateway de Internet y restaurarlo

Hacer copia de seguridad de su gateway de Internet le permite restaurar su estado original en caso de un error. Es posible realizar una restauración parcial si algunos archivos de la lista de copia de seguridad son inexistentes o están dañados. Es posible también realizar una restauración completa en caso de daños graves en la configuración del gateway de Internet. Por ejemplo, se ha reemplazado un disco duro en su equipo de gateway de Internet.

Es posible realizar una copia de seguridad sin detener el servicio de gateway de Internet.

Es necesario hacer copia de seguridad de los archivos en las carpetas dadas de la siguiente manera:

- Los archivos `openssl.cnf`, `server.crt` y `server.key` en la carpeta `C:\\Program Files\Symantec\SMP Internet Gateway\Apache\certs`
- Todos los archivos en la carpeta `C:\\Program Files\Symantec\SMP Internet Gateway\Apache\certs\client`
- Todos los archivos en la carpeta `C:\\Program Files\Symantec\SMP Internet Gateway\Apache\certs\crl`
- Todos los archivos en la carpeta `C:\\Program Files\Symantec\SMP Internet Gateway\Apache\conf`

Para realizar una restauración parcial

1. Abra **Administrador del gateway de Internet de Symantec Management Platform** y en la ficha **General**, en **Servicio de gateway de Internet**, haga clic en **Detener** para detener el servicio de gateway de Internet.
2. Restaure los elementos con problemas de la lista de copia de seguridad.
3. Abra **Administrador del gateway de Internet de Symantec Management Platform** y en la ficha **General**, en **Servicio de gateway de Internet**, haga clic en **Iniciar** para iniciar el servicio de gateway de Internet.

   Una vez que se inicia el servicio, asegúrese de que la configuración del gateway de Internet sea correcta y la funcionalidad esté funcionando correctamente.

Para realizar una restauración completa

1. Realice una nueva instalación del gateway de Internet.

   Al finalizar la instalación, anule la selección de **Iniciar el asistente de configuración**.
2. Restaure todos los elementos de la lista de copia de seguridad a las ubicaciones correspondientes en el equipo de gateway de Internet.
3. Abra el **Administrador del gateway de Internet de Symantec Management Platform** y en la ficha **Configuración**, haga clic en **Ejecutar el asistente**.
4. En el asistente **Configuración del gateway de Internet de Symantec Management Platform**, revise las páginas y asegúrese de que todos los datos se hayan completado correctamente.

5 En la página **Cuenta de usuario**, especifique los credenciales del servicio de gateway de Internet.

6 En la página **Resumen**, revise la configuración, asegúrese de que **¿Desea reiniciar los servicios automáticamente?** esté seleccionado y después haga clic **Terminar**.

Una vez que se inicia el servicio, asegúrese de que la configuración del gateway de Internet sea correcta y la funcionalidad esté funcionando correctamente.

Ver "Tareas de mantenimiento y solución de problemas habilitadas para la nube" en la página 327.

Visualización de informes de administración habilitada para la nube

Se proporciona un conjunto completo de informes para ayudarlo a supervisar y administrar sus equipos habilitados para la nube. Es posible también crear informes personalizados que se adapten a sus requisitos.

Ver "Creación y modificación de informes personalizados de Notification Server" en la página 452.

Para ver los informes de administración habilitada para la nube

1 En Symantec Management Console, en el menú **Informes**, haga clic en **Todos los informes**.

2 En el panel izquierdo, haga clic en **Informes > Administración de Notification Server > Agente > Administración habilitada para la nube** y, después, haga clic en el informe que desee ver.

Ver "Tareas de mantenimiento y solución de problemas habilitadas para la nube" en la página 327.

Sección 6

Cómo administrar recursos de Symantec Management Platform

- Capítulo 22. Configuración de la seguridad de recursos
- Capítulo 23. Configuración de filtros y destinos de recursos
- Capítulo 24. Configuración de paquetes
- Capítulo 25. Uso de directivas
- Capítulo 26. Usar las tareas y los trabajos
- Capítulo 27. Uso del Administrador de recursos
- Capítulo 28. Cómo usar los informes de Notification Server
- Capítulo 29. Cómo crear los informes personalizados de Notification Server
- Capítulo 30. Visualización de información del recurso

Capítulo 22

Configuración de la seguridad de recursos

En este capítulo se incluyen los temas siguientes:

- Configuración de la seguridad de recursos
- Consideraciones para el ámbito del recurso

Configuración de la seguridad de recursos

El modelo de seguridad del recurso ha cambiado perceptiblemente para los recursos de Notification Server 7.0., que incluyen todos los equipos, usuarios y todo lo demás que se defina en CMDB o el modelo del recurso, ahora obtienen todas sus concesiones de permisos de las vistas organizativas y de los grupos a los cuales pertenecen. Esto reemplaza la implementación de Notification Server 6.0, la cual precisa asegurar tanto las colecciones estándar y las carpetas de recursos.

Nota: Existen pocas excepciones, tales como paquetes, los cuales son recursos pero también son elementos que aparecen en la estructura de carpeta de Symantec Management Console. Las opciones de seguridad para estos elementos se deshabilitan en la estructura de carpeta. La seguridad para estos elementos se configura de la misma manera que para los otros recursos.

Una vista organizativa es un grupo jerárquico de recursos (como grupos organizativos) que refleja una vista o estructura real de su organización. Por ejemplo, puede crear vistas organizativas para agrupar sus recursos según ubicación geográfica, departamento o estructura de red. Como en el mundo real, un recurso puede (pero no es necesario) aparecer solamente una vez en una vista organizativa.

La asignación de recursos en grupos organizativos es automática y no se puede cambiar. Puede haber un retraso entre la detección del recurso y la muestra del mismo en el grupo organizativo apropiado. Cada recurso nuevo que ha sido detectado se coloca en el grupo organizativo de nivel superior y permanece allí hasta que se mueva al grupo organizativo apropiado cuando se ejecute la programación de actualización de la Vista organizativa.

Es posible eliminar recursos de cualquier vista organizativa, excepto de la vista **predeterminada**. Cuando un recurso se elimina de CMDB, se elimina automáticamente de todas las vistas organizativas usando la programación de actualización delta.

Ver "Programación de actualizaciones de pertenencia de recursos" en la página 367.

Se configura la seguridad asignando los permisos apropiados para cada rol de seguridad en cada vista organizativa y en los grupos organizativos dentro de cada vista. Un permiso que se asigna a un grupo organizativo se aplica a todos los recursos en ese grupo y de forma predeterminada a todos los grupos secundarios. No es posible asignar permisos directamente a un recurso determinado.

Las concesiones del permiso a un recurso se acumulan en las vistas organizativas. Los permisos con los que cuenta un rol de seguridad en un recurso en particular es la unión de todos los permisos que el recurso ha sido asignado mediante los grupos organizativos a los cuales pertenece. Si un rol de seguridad tiene permiso para llevar a cabo una acción en un recurso en una vista organizativa, tal rol puede realizar esa acción independientemente si el permiso se aplica a otras vistas organizativas que contienen el mismo recurso. Por ejemplo, si un rol de seguridad tiene acceso de lectura a un recurso en una vista organizativa, acceso de escritura al mismo recurso en otra vista organizativa pero no cuenta con acceso al recurso en una tercer vista organizativa, el rol tiene tanto el acceso de lectura como de escritura al recurso.

De esta manera, la implementación de la seguridad de recursos le otorga a cada rol de seguridad una vista única, o "ámbito", de los recursos disponibles. El rol de seguridad determina a qué recursos pueden acceder sus miembros y qué acciones pueden llevar a cabo en esos recursos. Los resultados de filtros, destinos e informes son dinámicos y automáticamente definidos según el rol del usuario que los posee. Por lo tanto, los resultados de filtros, destinos e informes contienen siempre solamente los recursos para los cuales ese usuario tiene los permisos de acceso necesarios.

Configurar la seguridad de recursos es un paso opcional en el proceso de configurar la seguridad de Symantec Management Platform.

Ver "Configuración de la seguridad de Symantec Management Platform" en la página 85.

Nota: Cuando se evalúa un destino, solamente se encuentran disponibles aquellos recursos para los cuales el usuario cuenta con permiso de lectura. En consecuencia, el único permiso de seguridad que el usuario precisa para aplicar una tarea o política a un recurso es el permiso de lectura en el recurso.

Tabla 22-1 Proceso para configurar la seguridad de recursos

Paso	Acción	Descripción
Paso 1	Identifique su administración de recursos y requisitos de seguridad.	Necesita determinar su administración de recursos y requisitos de seguridad y luego planear las estructuras de vistas organizativas de acuerdo a sus necesidades. Puede utilizar cualquier estructura que desee. Por ejemplo, puede utilizar vistas organizativas basadas en geografía, funciones comerciales o estructura de administración. Para obtener más información, consulte *Guía de implementación y planificación de IT Management Suite*.
Paso 2	Cree las vistas organizativas que desee.	Cree las vistas organizativas que precisa para modelar las estructuras lógicas apropiadas para su organización. Ver "Crear y configurar una vista organizativa" en la página 343. Ver "Crear y rellenar una vista o grupo organizativo" en la página 343.
Paso 3	En cada vista organizativa, cree los grupos organizativos que desee y asigna los recursos apropiados a cada grupo organizativo.	Dentro de cada vista organizativa, puede crear una jerarquía de grupos para representar la estructura organizativa que desea modelar. Los nuevos recursos se agregan de forma automática a la vista organizativa **predeterminada**. Puede moverlos a los grupos apropiados dentro de cada una de sus vistas organizativas. Ver "Crear y configurar un grupo organizativo" en la página 344. Ver "Recursos de la visualización en un grupo organizativo" en la página 345.
Paso 4	Asigne los roles de seguridad apropiados para cada grupo organizativo.	La asignación de un rol de seguridad a un grupo organizativo les otorga a los usuarios de ese rol acceso a todos los recursos que se incluyen directamente en ese grupo. Necesita especificar los permisos que cada rol tiene en el grupo. De forma predeterminada, la configuración de seguridad en un grupo aplica a todos sus grupos secundarios. Puede ponerle fin a la herencia cuando lo considere necesario. Ver "Configuración de la seguridad en un grupo organizativo" en la página 346.

Crear y configurar una vista organizativa

Una vista organizativa es un grupo jerárquico de recursos (como grupos organizativos) que refleja una vista o estructura real de su organización. Por ejemplo, puede crear vistas organizativas para agrupar sus recursos según ubicación geográfica, departamento o estructura de red. Como en el mundo real, un recurso puede (pero no es necesario) aparecer solamente una vez en una vista organizativa.

Las vistas organizativas proporcionan un medio seguro para segregar sus recursos en unidades bien estructuradas y administrables. Una vista organizativa no puede contener ningún recurso de forma directa - todos los recursos deben estar contenidos en grupos organizativos. Puede utilizar vistas y grupos organizativos para modelar una gran variedad de requisitos organizativos. Puede asegurar sus vistas organizativas utilizando el modelo de herencia de seguridad NT que se utiliza en la plataforma de administración Symantec.

Puede utilizar vistas y grupos organizativos dentro de los destinos cuando desea aplicar una directiva o tarea a los equipos seleccionados, usuarios o recursos. El grupo o la vista organizativos se usan de la misma forma que un filtro, pero proporciona, la seguridad que se necesita para asegurar de que solamente se incluyan aquellos recursos para los cuales el propietario de destino tiene permiso.

Esta tarea es un paso en el proceso para configurar la seguridad del recurso.

Ver "Configuración de la seguridad de recursos" en la página 340.

Para crear un grupo organizativo

1. En Symantec Management Console, en el menú **Administrar**, haga clic en **Vista y grupos organizativos**.
2. En el panel izquierdo, haga clic con el botón derecho en la carpeta **Vistas organizativas** y, después, haga clic en **Nueva > Vista organizativa**.
3. (Opcional) En el panel derecho, edite el nombre y la descripción de la vista organizativa.
4. Para especificar los grupos organizativos que se muestran, haga lo siguiente:
   - En el panel derecho, haga clic en **Filtro**.
   - En el cuadro de diálogo **Grupos visibles para el filtro**, compruebe los grupos organizativos que desee que estén visibles para esta vista organizativa y, después, haga clic en **Aceptar**.

Crear y rellenar una vista o grupo organizativo

En la vista mejorada **Equipos**, puede crear y rellenar fácilmente vistas y grupos organizativos.

Para crear y rellenar una vista o grupo organizativo

1. En Symantec Management Console, en el menú **Administrar**, haga clic en **Equipos**.
2. Haga clic con el botón derecho en **Vistas de todos los equipos** y haga clic en **Nueva > Vista organizativa**.
3. En el cuadro de diálogo **Vista organizativa**, escriba el nombre para la vista organizativa y después haga clic en **Aceptar**.
4. Haga clic con el botón derecho en la nueva vista organizativa y haga clic en **Nuevo > Grupo organizativo**.

   Tenga en cuenta que no puede agregar grupos organizativos a la vista organizativa predeterminada **Todos los equipos**.
5. En el cuadro de diálogo **Grupo organizativo**, escriba el nombre para el nuevo grupo y después haga clic en **Aceptar**.
6. Para rellenar al nuevo grupo organizativo, haga lo siguiente:
   - En **Vistas de todos los equipos**, haga clic en **Todos los equipos**.
   - En el panel de lista, seleccione los equipos que desea agregar a este grupo organizativo.
     Puede usar las teclas **Mayús** o **Ctrl** para seleccionar varios equipos.
   - Arrastre los equipos seleccionados al nuevo grupo organizativo o haga clic con el botón derecho en uno de los equipos seleccionados y después haga clic en **Agregar grupo organizativo**. En el cuadro de diálogo **Agregar grupo organizativo**, haga clic en el grupo al cual desea agregar los equipos y haga clic en **Aceptar**.

Crear y configurar un grupo organizativo

Cada vista organizativa contiene uno o más grupos organizativos y cada uno puede contener recursos y grupos organizativos secundarios. La estructura jerárquica de los grupos organizativos puede tener tantos niveles como necesite para representar la manera en la cual los recursos se organizan en su entorno. La pertenencia a un grupo organizativo incluye los recursos que están contenidos en todos los grupos secundarios.

Symantec Management Console tiene una vista organizativa **predeterminada** en la cual todos los recursos se colocan de forma automática. La estructura predeterminada es una jerarquía de grupos organizativos basada en un tipo de recurso. No es posible agregar o quitar grupos organizativos de la vista organizativa **predeterminada**. Todos los recursos que han sido detectados de forma reciente

se colocan automáticamente en el grupo apropiado en la vista organizativa **predeterminada**.

Esta tarea es un paso en el proceso para configurar la seguridad del recurso.

Ver "Configuración de la seguridad de recursos" en la página 340.

Para crear y configurar un grupo organizativo

1. En Symantec Management Console, en el menú **Administrar**, haga clic en **Vistas y grupos organizativos**.
2. En el panel izquierdo, haga clic con el botón derecho en la vista organizativa en la que desea agregar un grupo organizativo y después haga clic en **Nuevo > Grupo organizativo**.
3. En el panel derecho, edite el nombre y la descripción del grupo organizativo.

   Los nombres de los grupos no tienen restricciones, de modo que puede tener varios grupos con el mismo nombre.
4. Para agregar recursos al grupo, haga lo siguiente:
   - En el panel derecho, haga clic en **Agregar** y después haga clic en el elemento que desee agregar el grupo.
   - En el cuadro de diálogo **Editar grupo**, seleccione los recursos apropiados y después haga clic en **Aceptar**.
5. Para eliminar un recurso del grupo, haga clic con el botón derecho en el recurso y después haga clic en **Eliminar**.

Advertencia: Cuando se elimina un recurso, se lo elimina del CMDB. No es necesario eliminar ningún recurso que sea crítico para la actividad y las funciones de la Plataforma de administración Symantec. Los recursos críticos incluyen un equipo Notification Server, sitios y subredes.

Recursos de la visualización en un grupo organizativo

El panel Recursos muestra todos los recursos que están incluidos directamente en el grupo organizativo y todos los recursos que están incluidos en cualquiera de sus grupos secundarios. Es posible cambiar la vista para ver solamente los equipos que están en el grupo.

Ver "Configuración de la seguridad de recursos" en la página 340.

Es posible ver la lista de recursos que estén disponibles para un rol de seguridad determinado. Por ejemplo, se puede verificar que se haya configurado correctamente la seguridad del recurso para un rol determinado. Los roles de seguridad que se

asignan a un grupo organizativo determinan el acceso a todos los recursos que se incluyen directamente en ese grupo. Cada rol de seguridad tiene acceso solamente a los recursos que se incluyen directamente en los grupos a los que se asigna el rol.

Cuando se ven los recursos para un rol de seguridad determinado, se ven solamente los recursos que están disponibles para el rol seleccionado y su rol. Si su rol es el rol de administrador (que tiene acceso a todos los recursos), se ven siempre todos los recursos que están disponibles para el rol seleccionado. Sin embargo, si tiene otro rol (que pueda no tener acceso a todos los recursos), no se pueden ver todos los recursos que estén disponibles para el rol seleccionado.

Nota: Si no pertenece a un rol (es decir, la seguridad basada en usuarios se ha aplicado en lugar de basada en roles), elija **Ninguno** para no tener ningún rol de seguridad seleccionado. Esto garantiza que se muestren todos los recursos a los que tiene acceso. Si selecciona un rol al que usted no pertenece, todos los recursos se filtran y no verá nada.

Es posible realizar acciones de administración en recursos en un grupo organizativo. Las acciones incluyen abrir el Administrador de recursos, exportar el recurso a un archivo XML, ver las propiedades del recurso, agregar el recurso a un grupo diferente y eliminar el recurso del grupo.

Para ver recursos en un grupo organizativo

1. En Symantec Management Console, en el menú **Administrar**, haga clic en **Vistas y grupos organizativos**.
2. En el panel izquierdo, expanda la carpeta **Vistas organizativas** y después seleccione el grupo organizativo apropiado.
3. (Opcional) Para ver los recursos para un rol de seguridad determinado, en el panel derecho, en **Recursos**, en la lista desplegable **Rol**, haga clic en el rol apropiado.

Configuración de la seguridad en un grupo organizativo

Configura la seguridad en un grupo organizativo asignándole al grupo los roles de seguridad apropiados. Cuando se asigna un rol de seguridad a un grupo, los miembros de ese rol de seguridad tienen acceso a los recursos que están en el grupo. De manera predeterminada, todos los grupos secundarios heredan todas las asignaciones de seguridad en un grupo organizativo. La herencia otorga al rol el mismo acceso a todos los recursos en los grupos secundarios. Puede poner fin a la herencia en cualquier nivel y restaurarla cuando sea necesario.

Para configurar la seguridad en grupos organizativos, precisa el permiso de sistema Cambiar permisos.

Cuando instala la Symantec Management Platform, la configuración predeterminada establece que todos los roles tienen permiso completo en la vista organizativa **Predeterminada**. La configuración predeterminada otorga a todos los roles acceso completo a todos los recursos. Si desea configurar la seguridad de recursos (opcional), puede utilizar la vista organizativa **Predeterminado** para establecer los permisos predeterminados en todos los recursos o en tipos de recursos en particular. Necesita poner fin a la herencia para los roles de seguridad apropiados y borrar los permisos en la estructura de grupo organizativo.

Es posible entonces asignar un rol de seguridad a un grupo organizativo con los permisos que son apropiados para ese rol. Por ejemplo, el rol del administrador requerirá derechos de administración completos para todos los recursos en un grupo. Sin embargo, un rol de usuario final puede precisar solamente acceso de lectura para esos recursos. De manera predeterminada, la asignación de algunos permisos a un rol de seguridad en un grupo organizativo le otorga al rol los mismos permisos en todos sus grupos secundarios.

Esta tarea es un paso en el proceso para configurar la seguridad del recurso.

Ver "Configuración de la seguridad de recursos" en la página 340.

Para configurar la seguridad en un grupo organizativo

1. En Symantec Management Console, en el menú **Administrar**, haga clic en **Vistas y grupos organizativos**.
2. En el panel izquierdo, haga clic con el botón derecho en el grupo organizativo, haga clic en **Administrar seguridad** y, a continuación, realice una de las siguientes acciones:

Para asignar todos los permisos disponibles	■ Haga clic en **Asignar derechos de administración**. ■ En el cuadro de diálogo **Asignar derechos de administración**, seleccione los roles de seguridad apropiados y después haga clic en **Aceptar**.
Para asignar el permiso "Leer" del sistema de Symantec	■ Haga clic en **Asignar leído**. ■ En el cuadro de diálogo **Asignar derechos de lectura**, seleccione los roles de seguridad apropiados y, después, haga clic en **Aceptar**.

Para configurar los permisos de seguridad personalizados	■ Haga clic en **Asignar personalizado**. ■ En **Administrador de roles de seguridad**, en la lista desplegable **Rol**, haga clic en el rol de seguridad para el cual quiere establecer los permisos personalizados. ■ En la lista desplegable **Ver**, haga clic en **Todos los elementos**. ■ En el panel izquierdo, seleccione la vista o el grupo organizativo para el cual quiere establecer los permisos. ■ En el panel derecho, en **No heredado**, realice los cambios apropiados a la configuración de permisos. ■ (Opcional) Si desea configurar la herencia de permisos, haga clic en **Opciones avanzadas**. Ver "Personalización de permisos de herencia" en la página 104. ■ Haga clic en **Guardar cambios**.

3 Haga clic en **Guardar cambios**.

Consideraciones para el ámbito del recurso

El ámbito del recurso proporciona medios seguros de segregar recursos en unidades manejables y bien estructuradas. Estas unidades son de naturaleza genérica, de modo que se pueden organizar para adaptarse a una amplia variedad de requisitos organizativos.

En la mayoría de los casos, la evaluación de los requisitos de ámbito del recurso del diseño se reduce a las preguntas siguientes:

- ¿Quién debe tener acceso completo a la infraestructura de Symantec Management Platform?
- ¿Qué roles existen dentro de las funciones de administración de las operaciones diarias?
- ¿Qué áreas de funcionalidad necesitan roles y derechos específicos?
- ¿Active Directory refleja con exactitud nuestro modelo de administración y de negocio?
- ¿Existen grupos de Active Directory que reflejan los roles dentro de la arquitectura de Symantec Management Platform?
- ¿Qué tipos de recursos se necesitan administrar?

Cuando diseñe el marco del recurso, use la lista de control de implementación siguiente para garantizar que se complete en el orden correcto:

- Identifique usuarios, roles de seguridad y derechos.
- Cree roles de seguridad.
  Asigne derechos y asigne pertenencia a usuarios.
- Cree la estructura de grupos y vistas organizativos.
  Siga las prácticas recomendadas de importación de AD. Agrupe por tipo de recurso (usuario, equipo).
- Asigne los roles y los permisos a las vistas y los grupos organizativos específicos.
- Genere informes para la vista del sistema de línea base de recursos.
- Haga una copia de seguridad de la estructura de la vista y del grupo organizativos usando la exportación XML.

Tabla 22-2 Consideraciones de diseño para el ámbito del recurso

Elemento	Consideraciones de diseño
Seguridad	■ Es necesario configurar los roles de seguridad antes de realizar otras tareas de seguridad de la consola y antes de que Notification Server se implemente en el entorno de producción. ■ La seguridad del recurso es la combinación de ámbito, rol de seguridad y permisos. ■ Los recursos obtienen todas las concesiones de permiso de las colecciones de ámbitos de las que son miembro. Las concesiones son acumulativas por naturaleza. Teniendo permiso para realizar una acción en un recurso de una colección de ámbitos, se asegura de que el usuario/rol pueda continuar realizando esa acción sin importar si el permiso se aplica a otras colecciones de ámbitos que contienen el recurso. ■ Los roles de seguridad son grupos de usuarios que permiten asignar privilegios para las responsabilidades administrativas y de trabajadores, y permisos para las carpetas o los elementos que los administradores y los trabajadores pueden consultar en Symantec Management Console. ■ Los roles listos para usar se proporcionan con una variedad de concesiones de privilegios y se pueden asignar en cualquier lugar dentro de la estructura de la vista organizativa o del grupo organizativo, según el ámbito administrativo que se elige conceder. ■ Las concesiones de seguridad se asignan a los grupos organizativos y se heredan del grupo organizativo que está un nivel superior.

Elemento	Consideraciones de diseño
Vistas organizativas	■ Una vista organizativa es una jerarquía segura y autónoma de grupos organizativos que contienen recursos. ■ Las vistas organizativas proporcionan un medio simplificado y seguro de agrupar y administrar recursos. ■ Considere una vista organizativa para representar un límite o una estructura de seguridad administrativa que se alinee con el entorno de TI. ■ Duplique el modelo organizativo de Active Directory mediante la importación de Active Directory para evitar el relleno y la creación manual. ■ Todos los recursos en una vista organizativa (administrada y no administrada) se definen de forma predeterminada. ■ Las vistas organizativas contienen solamente recursos por medio de grupos organizativos. Una vista organizativa no puede contener ningún recurso directamente. Todos los recursos recientemente detectados se importan de forma automática a la vista organizativa predeterminada. ■ Un elemento de recursos puede pertenecer solamente a un grupo organizativo en cada vista organizativa. Cuando agrega un recurso a un grupo organizativo, se elimina automáticamente de cualquier otro grupo al que puede estar asignado. ■ Use grupos organizativos para aplicar una política o una tarea a equipos, usuarios y recursos seleccionados. Para hacer esto, use un grupo organizativo en un destino. En esta instancia, un grupo organizativo funciona como filtro, pero proporciona seguridad para garantizar que solo se incluya el recurso al que el propietario de destino tiene permiso. ■ Symantec Management Platform permite varias vistas organizativas porque los administradores pueden tener varias maneras de organizar los recursos. Por lo tanto, puede tener una vista por función y por región. ■ Con la vista organizativa predeterminada, todos los recursos se definen y protegen en esta vista; los recursos (administrados y no administrados) se agrupan por tipo; y la pertenencia a recursos es dinámica. ■ La pertenencia a recursos dentro de la vista predeterminada del sistema se actualiza dinámicamente y se configura en un intervalo de actualización de 5 minutos. Según cómo planea la creación y la pertenencia a recursos de la estructura organizativa, recuerde este problema al identificar el impacto general de las actualizaciones de la pertenencia a recursos.

Elemento	Consideraciones de diseño
Filtros	■ Los filtros son conceptualmente similares a las colecciones de Notification Server 6. Se implementan de manera diferente debido a que se aplican a los destinos, no a las políticas. Son recursos asociados por un conjunto definido de criterios. ■ Los filtros se deben crear a partir de un único atributo. Los filtros se pueden combinar para crear destinos complejos, y usando menos criterios, se obtiene una mayor posibilidad de reutilización y una menor complejidad, lo que da lugar a un Notification Server más eficaz.
Destinos	■ Los destinos son la intersección de los grupos organizativos y los filtros. Por ejemplo, todos los equipos en Finanzas (grupo) que tienen menos de 1 GB de RAM (filtro). ■ Los destinos se aplican a políticas y tareas, y pueden crearse previamente o en el momento de aplicación. ■ Los destinos pueden contener solamente los recursos a los que el creador de destino tiene acceso. No son visibles como objetos en la consola, pero son accesibles usando la opción **Aplicar rápidamente en** en una tarea o una política.

Capítulo 23

Configuración de filtros y destinos de recursos

En este capítulo se incluyen los temas siguientes:

- Acerca de los filtros de recursos
- Creación o modificación de un filtro
- Ejecución de acciones en recursos de filtros
- Visualización de las dependencias de filtro
- Acerca de los destinos de recursos
- Programación de actualizaciones de pertenencia de recursos

Acerca de los filtros de recursos

Un filtro, también conocido como filtro de recursos, es una definición dinámica de un conjunto de recursos. Los recursos se pueden agrupar según algunos parámetros especificados y también se los puede excluir explícitamente de un filtro o se los puede incluir en él. Por lo general, un filtro aísla solamente un aspecto de un recurso, como su sistema operativo, espacio disponible en el disco o RAM. Los filtros se utilizan con grupos organizativos para identificar los recursos (un recurso de destino) a los cuales se aplican una tarea o una política.

Ver "Acerca de los destinos de recursos" en la página 366.

Un filtro no contiene ningún recurso específico. Los recursos están incluidos en grupos organizativos, configurados en vistas organizativas. Los grupos organizativos y las vistas organizativas son los mismos que se usan para la seguridad del recurso. Un filtro funciona en una vista o un grupo organizativo específico para identificar los recursos adecuados. Por lo tanto, los filtros son portátiles y se pueden aplicar

a cualquier vista o grupo organizativo, y se los puede usar con otros filtros. Por ejemplo, se puede aplicar una política a todos los equipos con Windows XP en un departamento determinado de la organización. En este caso, para seleccionar solamente los equipos con Windows XP, puede aplicar un filtro al grupo organizativo que representa al departamento apropiado.

Ver "Creación o modificación de un filtro" en la página 354.

Creación o modificación de un filtro

Es posible crear un nuevo filtro desde el comienzo, o bien clonar un filtro existente y modificarlo para que se adapte a sus requisitos. Puede modificar cualquier filtro que haya creado o cualquier filtro en el que tiene permiso de escritura. Sin embargo, no es posible modificar los filtros predeterminados que se proporcionan con Notification Server. No es posible modificar ninguno de los filtros que agregue la réplica de la jerarquía desde el Notification Server principal. Solamente los filtros creados en su Notification Server pueden editarse de forma local.

Ver "Acerca de los filtros de recursos" en la página 353.

Es posible también crear un filtro al guardar un informe. Un filtro creado de esta manera es un filtro estático y no tiene ninguna consulta. La pertenencia al filtro es una lista fija de inclusiones que se determina cuando se crea el filtro. Es posible modificar un filtro estático agregando más inclusiones o exclusiones, que pueden ser filtros dinámicos. Sin embargo, no se puede agregar una consulta directamente a un filtro estático.

Ver "Cómo crear un filtro estático a partir de resultados del informe de Notification Server" en la página 447.

Tabla 23-1 Proceso para crear o modificar un filtro

Paso	Acción	Descripción
Paso 1	Cree un filtro nuevo o seleccione el filtro existente que desea modificar.	Es posible crear un nuevo filtro desde el comienzo o modificar un filtro existente para que se adapte a sus requisitos. Ver "Creación de un nuevo filtro" en la página 355. Ver "Modificación de un filtro existente" en la página 356.
Paso 2	Seleccione el tipo de consulta.	Este paso se aplica solamente a un filtro nuevo. No es posible cambiar el tipo de consulta cuando se modifica un filtro existente. Si desea crear un filtro dinámico, es necesario seleccionar el tipo de consulta apropiado. Si no elige ninguna consulta, la pertenencia al filtro serán las inclusiones y las exclusiones especificadas. Ver "Selección del tipo de consulta del filtro" en la página 357.

Paso	Acción	Descripción
Paso 3	Especifique la consulta que desea usar.	Puede escribir la consulta SQL usted mismo o usar la Generación de consultas para generar la consulta del filtro. El Generador de consultas es una herramienta fácil de usar que le permite seleccionar las tablas y los campos que desea usar. Lo ayuda a definir la consulta para que se adapte a sus requisitos. Ver "Cómo definir una consulta de recursos para un filtro" en la página 358. Ver "Cómo definir una consulta SQL para un filtro" en la página 360.
Paso 4	Especifique las inclusiones y las exclusiones.	Es posible especificar recursos o filtros determinados para incluir o excluir en el filtro. Los filtros que se incluyen o se excluyen pueden contener otros filtros. Puede seleccionar los recursos y los filtros que están disponibles en la CMDB, y puede importar recursos de un archivo CSV. Ver "Especifique las inclusiones y las exclusiones de filtro." en la página 361.
Paso 5	Verifique la configuración del filtro. Para ello, consulte la pertenencia al filtro.	La pertenencia de un filtro se determina mediante la ejecución de la consulta del filtro en la CMDB para extraer los recursos apropiados. Es posible actualizar la pertenencia al filtro para verificar que el filtro esté definido correctamente. Ver "Actualización de la pertenencia a un filtro" en la página 363.
Paso 6	Guarde el filtro.	Es posible guardar la definición del filtro nueva o modificada. Un vez guardado el nuevo filtro, no se puede cambiar su tipo de consulta. Ver "Creación de un nuevo filtro" en la página 355. Ver "Modificación de un filtro existente" en la página 356.

Creación de un nuevo filtro

Es posible crear todos los filtros nuevos que se necesiten, así como especificar la consulta, las inclusiones y las exclusiones deseadas para definir la pertenencia.

Ver "Acerca de los filtros de recursos" en la página 353.

Esta tarea es un paso en el proceso para crear o modificar un filtro.

Ver "Creación o modificación de un filtro" en la página 354.

Para crear un nuevo filtro

1. En Symantec Management Console, en el menú **Administrar**, haga clic en **Filtros**.
2. En el panel izquierdo, haga clic con el botón derecho en la carpeta en la que desea agregar el nuevo filtro y, a continuación, haga clic en **Nuevo > Filtro**.
3. En el panel derecho, especifique el nombre y la descripción del filtro.
4. Seleccione el tipo de consulta.

   Ver "Selección del tipo de consulta del filtro" en la página 357.
5. Realice una de las siguientes acciones:

Defina la consulta	Ver "Cómo definir una consulta de recursos para un filtro" en la página 358. Ver "Cómo definir una consulta SQL para un filtro" en la página 360.
Especifique todas las inclusiones y las exclusiones necesarias	Ver "Especifique las inclusiones y las exclusiones de filtro." en la página 361.
Actualice la pertenencia al filtro	Ver "Actualización de la pertenencia a un filtro" en la página 363.

6. Haga clic en **Guardar cambios**.

Modificación de un filtro existente

Puede modificar cualquier filtro que haya creado o cualquier filtro en el que tiene permiso de escritura. Sin embargo, no es posible modificar los filtros predeterminados que se proporcionan con Notification Server. No es posible modificar ningún filtro que sea añadido por la réplica de la jerarquía desde Notification Server principal. Solamente los filtros creados en su Notification Server pueden editarse de forma local. La única acción que se puede realizar en un filtro de sólo lectura es actualizar la pertenencia al filtro.

Ver "Acerca de los filtros de recursos" en la página 353.

Si desea modificar un filtro de sólo lectura, clónelo para crear un filtro nuevo y después modifíquelo para adaptarse a sus requisitos. Cuando se modifica un filtro, se puede modificar la consulta del filtro y las inclusiones o exclusiones específicas, pero no se puede cambiar el tipo de consulta.

Esta tarea es un paso en el proceso para crear o modificar un filtro.

Ver "Creación o modificación de un filtro" en la página 354.

Para modificar un filtro existente

1. En Symantec Management Console, en el menú **Administrar**, haga clic en **Filtros**.
2. En el panel izquierdo, haga clic en el filtro que desea modificar.
3. (Opcional) En el panel derecho, cambie el nombre del filtro y la descripción.
4. En la esquina superior derecha, haga clic en **Editar**.

   Si la opción Editar no está disponible, el filtro es de sólo lectura y no se puede modificar.
5. Realice una de las siguientes acciones:

Modifique la consulta	Ver "Cómo definir una consulta de recursos para un filtro" en la página 358. Ver "Cómo definir una consulta SQL para un filtro" en la página 360.
Modifique las inclusiones y las exclusiones	Ver "Especifique las inclusiones y las exclusiones de filtro." en la página 361.
Actualice la pertenencia al filtro	Ver "Actualización de la pertenencia a un filtro" en la página 363.

6. Haga clic en **Guardar cambios**.

Selección del tipo de consulta del filtro

Cuando se crea un nuevo filtro, es necesario especificar el tipo de consulta que se desea usar. Puede usar la Generación de consultas para definir la consulta del filtro, o bien puede escribir la consulta SQL usted mismo. Es posible también elegir que no desea tener ninguna consulta en el filtro. No es posible cambiar el tipo de consulta una vez que el filtro se guardó.

Ver "Acerca de los filtros de recursos" en la página 353.

Esta tarea es un paso en el proceso para crear o modificar un filtro.

Ver "Creación o modificación de un filtro" en la página 354.

Para seleccionar el tipo de consulta del filtro

1. En Symantec Management Console, en el menú **Administrar**, haga clic en **Filtros**.
2. En el panel izquierdo, haga clic con el botón derecho en la carpeta en la que desea agregar el nuevo filtro y, a continuación, haga clic en **Nuevo > Filtro**.
3. En la página **Filtro nuevo**, en la lista desplegable **Definición de filtro**, seleccione el tipo de consulta que desee usar:

Ninguno(a)	El filtro no usa una consulta. Las inclusiones y las exclusiones de recursos y de filtros específicos definen la pertenencia al filtro.
Generación de consultas	Use la Generación de consultas para generar la consulta del filtro. La Generación de consultas es una herramienta fácil de usar que le permite seleccionar las tablas y los campos que desea usar. Lo ayuda a definir la consulta para que se adapte a sus requisitos. Ver "Cómo definir una consulta de recursos para un filtro" en la página 358.
Consulta SQL sin procesar	Escriba su propia consulta SQL. Por ejemplo, puede copiar una consulta de otro filtro o informe y modificarla para que se adapte a sus requisitos. Ver "Cómo definir una consulta SQL para un filtro" en la página 360.

Cómo definir una consulta de recursos para un filtro

Una consulta de recurso se basa en las tablas disponibles en la CMDB. La Generación de consultas es una herramienta fácil de usar que proporciona una plantilla estándar y le permite seleccionar las tablas y los campos que desea usar. Lo ayuda a definir la consulta para que se adapte a sus requisitos. No necesita ningún conocimiento sobre SQL para definir una consulta de recurso. La consulta de recurso se convierte en SQL automáticamente, y SQL se ejecuta en la CMDB para extraer los recursos apropiados.

Ver "Selección del tipo de consulta del filtro" en la página 357.

Esta tarea es un paso en el proceso para crear o modificar un filtro.

Ver "Creación o modificación de un filtro" en la página 354.

Para definir una consulta de recursos para un filtro

1 En Symantec Management Console, en el menú **Administrar**, haga clic en **Filtros**.

2 En el panel izquierdo, haga clic en el filtro que desea modificar.

3 En el panel derecho, en el panel **Definición de filtro**, especifique los detalles de la consulta de recursos en las fichas apropiadas.

Consulta	La sintaxis de la consulta de recurso. Ver "Página Edición de informes personalizada: ficha Origen de datos, ficha Consulta " en la página 529.
Campos	Campos y atributos de clase de datos que se usan en la consulta. Ver "Página Edición de informes personalizada: ficha Origen de datos, ficha: Campos " en la página 532.
Parámetros de consulta	Los parámetros que se usan en la consulta. Éstos son parámetros internos para el uso de SQL, no parámetros de usuario. Parámetros que no se usan con frecuencia en las consultas de filtro, pero que pueden ser útiles para obtener información del registro. Por ejemplo, el número de versión de un agente para una actualización. Ver "Página Edición de informes personalizada: ficha Origen de datos, ficha Parámetros de consulta " en la página 534.
Expresiones de filtro	Las instrucciones condicionales que se usan para restringir más los resultados de la consulta. Cada instrucción o instrucción agrupada se puede considerar un filtro. Es necesario crear las instrucciones que desee usar y agruparlas como corresponda. Ver "Página Edición de informes personalizada: ficha Origen de datos, ficha: Expresiones de filtro " en la página 535.
Consulta resuelta	El código SQL que se ejecuta en CMDB para extraer los resultados del filtro. Ver "Página Edición de informes personalizada: ficha Origen de datos,, ficha: Consulta resuelta " en la página 537.

Cómo definir una consulta SQL para un filtro

Es posible escribir una consulta SQL para definir los recursos que desee incluir en el filtro. Es posible escribir el código SQL desde el comienzo. Como alternativa, puede copiar el código SQL de otro filtro o informe y modificarlo para que se adapte a sus requisitos. Por ejemplo, se puede crear una consulta de recursos con la Generación de consultas y después copiar el código SQL generado de la ficha Consulta resuelta. También puede usar la Generación de consultas para definir la estructura básica de la consulta, convertirla a SQL y después modificar la consulta SQL directamente para crear la consulta que desee.

Se necesita el privilegio de edición de SQL para crear o modificar consultas SQL. También es necesario tener una buena comprensión de la estructura de tablas de la CMDB.

Ver "Selección del tipo de consulta del filtro" en la página 357.

Esta tarea es un paso en el proceso para crear o modificar un filtro.

Ver "Creación o modificación de un filtro" en la página 354.

Para definir una consulta SQL para un filtro

1. En Symantec Management Console, en el menú **Administrar**, haga clic en **Filtros**.
2. En el panel izquierdo, haga clic en el filtro que desea modificar.

3 En el panel derecho, en el panel **Definición de filtro**, especifique los detalles de la consulta SQL en las fichas apropiadas.

Consulta con parámetros	El código SQL de la consulta. Ver "Página Edición de informes personalizada: ficha Origen de datos, ficha Consulta con parámetros " en la página 533.
Parámetros de consulta	Los parámetros que se usan en la consulta. Éstos son parámetros internos para el uso de SQL, no parámetros de usuario. Parámetros que no se usan con frecuencia en las consultas de filtro, pero que pueden ser útiles para obtener información del registro. Por ejemplo, el número de versión de un agente para una actualización. Ver "Página Edición de informes personalizada: ficha Origen de datos, ficha Parámetros de consulta " en la página 534.
Consulta resuelta	El código SQL que se ejecuta en CMDB para extraer los resultados del filtro. Ver "Página Edición de informes personalizada: ficha Origen de datos,, ficha: Consulta resuelta " en la página 537.

4 Haga clic en **Guardar cambios**.

Especifique las inclusiones y las exclusiones de filtro.

Es posible especificar recursos o filtros determinados para incluir o excluir en el filtro. Los filtros que se incluyen o se excluyen pueden contener otros filtros. Es posible seleccionar los recursos y los filtros de la lista de elementos disponibles en la CMDB y puede también importar recursos de un archivo .csv.

Si importa recursos de un archivo .csv, el archivo puede identificar un equipo por nombre, nombre de dominio completo o dirección IP. Se omite cualquier elemento que no se encuentra en la CMDB.

La pertenencia al filtro es determinada mediante la incorporación de inclusiones en los resultados de la consulta y la eliminación de las exclusiones. Los filtros y los recursos no tienen ninguna diferencia de prioridad.

Esta tarea es un paso en el proceso para crear o modificar un filtro.

Ver "Creación o modificación de un filtro" en la página 354.

Para especificar recursos para incluir o excluir

1. En Symantec Management Console, en el menú **Administrar**, haga clic en **Filtros**.
2. En el panel izquierdo, haga clic en el filtro que desea modificar.
3. En el panel derecho, en el panel de **Definición de filtro**, en **Exclusiones e inclusiones explicitas**, realice una de las siguientes acciones:

Para incluir recursos seleccionados	1 En **Inclusiones**, haga clic en **Seleccionar un recurso**. 2 En la ventana **Seleccionar recursos**, seleccione los recursos que desea incluir y haga clic en **Aceptar**.
Para incluir los recursos que se detallan en un archivo	1 En **Inclusiones**, haga clic en **Importar de un archivo**. 2 En la ventana **Seleccionar archivo para importar**, seleccione el archivo .CSV apropiado y, luego, haga clic en **Abrir**.
Para excluir recursos seleccionados	1 En **Exclusiones**, haga clic en **Seleccionar un recurso**. 2 En la ventana **Seleccionar recursos**, seleccione los recursos que desea excluir y haga clic en **Aceptar**.
Para excluir los recursos que se detallan en un archivo	1 En **Exclusiones**, haga clic en **Importar de un archivo**. 2 En la ventana **Seleccionar archivo para importar**, seleccione el archivo .CSV apropiado y, luego, haga clic en **Abrir**.

Se detallan los recursos seleccionados junto a los campos apropiados.

Para especificar filtros para incluir o excluir

1. En Symantec Management Console, en el menú **Administrar**, haga clic en **Filtros**.
2. En el panel izquierdo, haga clic en el filtro que desea modificar.
3. En el panel derecho, en el panel de **Definición de filtro**, en **Exclusiones e inclusiones explicitas**, realice una de las siguientes acciones:

Para incluir los filtros seleccionados	1 En **Inclusiones**, haga clic en **Seleccionar un filtro**. 2 En la ventana **Seleccionar filtros**, seleccione los filtros que desea incluir y haga clic en **Aceptar**.
Para excluir los filtros seleccionados	1 En **Exclusiones**, haga clic en **Seleccionar un filtro**. 2 En la ventana **Seleccionar filtros**, seleccione los filtros que desea excluir y haga clic en **Aceptar**.

Se detallan los filtros seleccionados junto a los campos apropiados.

Actualización de la pertenencia a un filtro

La pertenencia de un filtro se determina mediante la ejecución de la consulta del filtro en la CMDB para extraer los recursos apropiados. Para mantener la pertenencia al filtro actualizada a medida que la información del recurso en CMDB cambia, es necesario actualizar la pertenencia en los intervalos convenientes. Es posible usar las actualizaciones programadas del filtro para actualizar la pertenencia al filtro o se puede ejecutar la actualización manualmente en las horas apropiadas. Por ejemplo, cuando se crea o modifica un filtro, se puede actualizar la pertenencia para verificar que el filtro esté definido correctamente.

Ver "Acerca de los filtros de recursos" en la página 353.

Ver "Programación de actualizaciones de pertenencia de recursos" en la página 367.

El panel Pertenencia al filtro en la página *Nombre de filtro* muestra los detalles de los recursos en su ámbito que se identifican actualmente como miembros del filtro. La pertenencia al filtro puede ser diferente para diversos roles de usuario. Solamente los recursos sobre los que un usuario tiene permiso de lectura son visibles para ese usuario. Sin embargo, cuando un usuario actualiza manualmente la pertenencia a un filtro, la consulta del filtro se ejecuta en todos los recursos en CMDB. La consola restringe los resultados para mostrar solamente los recursos que están dentro del ámbito de visualización del usuario.

Esta tarea es un paso en el proceso para crear o modificar un filtro.

Ver "Creación o modificación de un filtro" en la página 354.

Para actualizar la pertenencia de un filtro

1. En Symantec Management Console, en el menú **Administrar**, haga clic en **Filtros**.
2. En el panel izquierdo, haga clic en el filtro cuya pertenencia desea actualizar.
3. En el panel derecho, en el panel **Pertenencia al filtro**, realice una de las siguientes acciones:

Para actualizar la pertenencia al filtro de forma inmediata	Haga clic en **Actualizar pertenencia**.
Para actualizar la pertenencia al filtro usando las programaciones de actualización del filtro	Haga clic en **Actualizar pertenencia> Automático**.
Para permitir actualizaciones manuales de la pertenencia al filtro solamente	Haga clic en **Actualizar pertenencia> Manual**. Esta opción desactiva las actualizaciones programadas para la pertenencia al filtro. Por ejemplo, el filtro contiene una consulta compleja que se desea ejecutar solamente cuando sea necesario.

Ejecución de acciones en recursos de filtros

Es posible realizar acciones en los recursos de filtros seleccionados. Estas opciones son las mismo que las que están disponibles en el menú contextual (haga clic con el botón derecho). Las acciones disponibles dependen del tipo de recurso que se seleccione, de modo que es posible que algunas opciones no estén disponibles para los recursos.

Ver "Acerca de los filtros de recursos" en la página 353.

Para realizar una acción en un recurso de filtro

1. En Symantec Management Console, en el menú **Administrar**, haga clic en **Filtros**.
2. En el panel izquierdo, haga clic en el filtro que desea utilizar.

3 En el panel derecho, en el panel **Pertenencia al filtro**, seleccione el recurso en el cual desee realizar una acción.

4 Haga clic en **Acciones** y después haga clic en la opción apropiada.

Administrador de recursos	Abre al recurso en la consola del Administrador de recursos.
Exportar	Exporta el recurso a un archivo XML.
Propiedades	Muestra las propiedades del recurso.
Establecer el estado del activo > Activo	Configura el estado de un activo como Activo. Esta configuración es relevante para la solución Asset.
Establecer el estado del activo > Retirado	Configura el estado de un activo como Retirado. Esta configuración es relevante para la solución Asset.
Agregar grupo organizativo	Asignar el recurso a un grupo organizativo.
Eliminar	Elimine el recurso del filtro.
Tarea de administración de energía	Programe o ejecute la tarea de administración de energía.

Visualización de las dependencias de filtro

Antes de modificar un filtro, se recomienda averiguar qué otros elementos dependen de él. Es posible ver una lista de todos los filtros, destinos, tareas y directivas que usan un filtro determinado.

Ver "Acerca de los filtros de recursos" en la página 353.

La lista de dependencias contiene todos los destinos que incluyen el filtro especificado directamente o dentro de un filtro incluido. La lista además contiene todas las directivas y tareas que se aplican a esos destinos. La inclusión del filtro en el destino define la dependencia. La dependencia no significa necesariamente que la directiva o la tarea está aplicada actualmente a un recurso del filtro.

Para ver las dependencias de un filtro

1 En Symantec Management Console, en el menú **Administrar**, haga clic en **Filtros**.

2 En el panel izquierdo, haga clic en el filtro para el cual desee ver las dependencias.

3 En el panel derecho, en el panel **Pertenencia al filtro**, haga clic en **Referenciado por**.

4 En el cuadro de diálogo **Elementos aplicados a este filtro**, consulte la lista de filtros, destinos, tareas y directivas que usan el filtro.

5 Haga clic en **Cerrar**.

Acerca de los destinos de recursos

Un destino de recursos, generalmente conocido como destino, es un marco que permite aplicar tareas y directivas a una colección dinámica de recursos. Un destino consta de, al menos, una vista o grupo organizativo y una cantidad de filtros. Los filtros restringen los recursos disponibles a fin de identificar los que desea. La vista o el grupo organizativo funcionan como filtro de seguridad. Garantizan que la directiva o la tarea se apliquen solamente a los recursos para los cuales el usuario cuenta con un rol de seguridad que le permite trabajar.

Ver "Especificación de destinos de una política o tarea" en la página 379.

Los destinos se almacenan en la memoria caché de CMDB y se evalúan de forma dinámica cuando se ejecuta la directiva o la tarea. El destino se evalúa en relación con el ámbito del usuario actual. Solamente se devuelven los recursos que aparecen en la vista o el grupo organizativo y en los filtros. El destino incluye solamente los recursos para los cuales el usuario tiene acceso de escritura. Los recursos que estén fuera del ámbito del usuario nunca son visibles.

Los filtros del sistema que se suministran con Notification Server contienen solamente recursos administrados, pero es posible que los destinos y las vistas y los grupos organizativos contengan recursos no administrados. También es posible crear filtros personalizados propios que incluyan recursos no administrados. Sin embargo, cuando se aplica un destino a una directiva o tarea, solamente los equipos administrados del destino pueden solicitar la directiva o ejecutar la tarea.

Hay dos tipos de destinos que se pueden aplicar a una directiva o a una tarea:

Destinos de recursos generados automáticamente	Son los destinos que no se han nombrado ni se han guardado explícitamente . Los destinos generados automáticamente se usan solamente por la directiva o la tarea en las cuales se crean. Por ejemplo, si se usa la opción Aplicar rápidamente en para seleccionar un filtro o el cuadro de diálogo Seleccionar recursos para seleccionar un conjunto de recursos, el destino correspondiente se crea y se añade a la directiva o a la tarea. Al destino generado automáticamente se le da un nombre predeterminado que se basa en el grupo organizativo, el filtro o el conjunto de recursos que lo contiene. Es posible editar estos destinos cuando se modifica la directiva o la tarea, pero no se puede aplicarlos a ninguna otra directiva o tarea.
Destinos de recursos con nombre	Son los destinos que se han guardado explícitamente como destinos de recursos con nombre. Los destinos con nombre se pueden aplicar a cualquier cantidad de tareas y directivas, y pueden ser modificados por cualquier usuario que tenga los permisos apropiados.

Ver "Acerca de los filtros de recursos" en la página 353.

Ver "Creación o modificación de un filtro" en la página 354.

Programación de actualizaciones de pertenencia de recursos

Es posible mantener actualizados todos los filtros de recursos, los grupos organizativos y los destinos del recurso mediante la configuración de programaciones de actualización del filtro apropiadas. Estas programaciones permiten actualizar los filtros, los grupos organizativos y los destinos necesarios en los intervalos correspondientes. Estas programaciones ayudan a administrar la carga de procesamiento que se impone a Notification Server.

Ver "Acerca de los filtros de recursos" en la página 353.

Symantec Management Platform incluye programaciones de actualización de pertenencia a recursos predefinidas. Estas programaciones son convenientes para muchos usos y no debería ser necesario modificarlas. Sin embargo, como los requisitos de su organización cambian, se pueden realizar los cambios necesarios.

Tabla 23-2 Programaciones de actualización de pertenencia a recursos

Programación	Descripción
Programación de actualización delta	Actualiza la pertenencia en los siguientes casos: ■ Filtros cuya pertenencia se ha modificado desde la última actualización. ■ Todos los grupos organizativos dinámicos. ■ Todos los destinos no válidos. Un destino se puede invalidar según los siguientes eventos: ■ Se guarda su definición. ■ Se modifica la pertenencia de un filtro en uso. ■ Se modifica la pertenencia de un grupo organizativo en uso. ■ Se modifica la seguridad que se aplica a un grupo organizativo en uso. De forma predeterminada, esta programación se ejecuta cada cinco minutos.
Programación de actualización completa	Reconstruye totalmente la pertenencia de todos los filtros, los grupos organizativos y los destinos, sin importar el estado del inventario o las modificaciones a las políticas. La actualización completa puede imponer una carga significativa en Notification Server y se debe programar según corresponda. De forma predeterminada, se programa una vez al día.
Programación de actualización de políticas	Actualiza la pertenencia de los filtros que utiliza una política si ésta se ha modificado desde la última actualización. Esta programación garantiza que, cuando se actualiza o se crea una política, todos los filtros incluidos en los destinos de política nueva o modificada se actualicen automáticamente. De forma predeterminada, esta programación se ejecuta cada cinco minutos.

Ver "Componentes de una programación de Symantec Management Platform" en la página 119.

Ver "Visualización del calendario interno de programaciones de Notification Server" en la página 124.

Para configurar las programaciones de actualización de pertenencia a recursos

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Notification Server > Actualización de pertenencia a recursos**.
2. En la página Actualización de pertenencia a recursos, configure las programaciones de actualización que desee usar.

   Ver "Cómo especificar una programación de política" en la página 387.
3. Si desea ejecutar una programación de actualización de forma inmediata, en el panel apropiado, haga clic en **Ejecutar**.

   Por ejemplo, puede asegurarse de que todos los cambios a los filtros surtan efecto de forma inmediata, en lugar de que se apliquen durante la actualización programada.
4. Haga clic en **Aceptar**.

Capítulo 24

Configuración de paquetes

En este capítulo se incluyen los temas siguientes:

- Cómo cambiar la configuración de un paquete
- Cómo actualizar los puntos de distribución de un paquete
- Habilitación del acceso a un paquete en una ubicación UNC de origen
- Cómo administrar programas del paquete

Cómo cambiar la configuración de un paquete

Un paquete incluye un conjunto de archivos que se pueden entregar a un recurso administrado. Por ejemplo, el paquete de Symantec Management Agent incluye el archivo AeXClientUpgrade.exe. El archivo AeXClientUpgrade.exe instala el agente en los recursos administrados.

La página **Paquete** permite configurar los valores del paquete, tales como origen del paquete, ubicación del paquete y cómo ejecutar el paquete.

Para cambiar la configuración de un paquete

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Todas las configuraciones**.
2. En el panel izquierdo, seleccione el paquete que desee modificar.

3 En la página **Paquete**, realice los cambios de configuración necesarios en las fichas apropiadas:

Paquete	
Programas	Ver "Cómo administrar programas del paquete" en la página 373.
Package Servers	
Opciones avanzadas	

4 Haga clic en **Guardar cambios** para confirmar la nueva configuración.

Necesitará actualizar los puntos de distribución de paquetes para actualizar la información de paquete en cada servidor de paquetes.

Ver "Cómo actualizar los puntos de distribución de un paquete" en la página 371.

Cómo actualizar los puntos de distribución de un paquete

Los puntos de la distribución de paquetes son las ubicaciones en donde se almacena el paquete, por ejemplo ubicaciones de servidores de paquetes o de origen UNC. La información de cada paquete se encuentra en un archivo XML que se almacena con el paquete. Esta información se debe actualizar cada vez que se modifica el paquete. Notification Server y los servidores de paquetes usan esta información para proporcionar los archivos apropiados cuando un equipo administrado solicita el paquete. La información del paquete se actualiza según una programación, pero se puede realizar una actualización manual cuando sea necesario. Por ejemplo, puede actualizar manualmente los puntos de distribución para que un paquete modificado actualice de forma inmediata la información del paquete en todos los puntos de distribución.

Ver "Cómo cambiar la configuración de un paquete" en la página 370.

Es posible actualizar los puntos de distribución de un paquete en el catálogo de software o de un paquete al que se accede desde el menú **Configuración**.

Para actualizar los puntos de la distribución de paquetes de un paquete del catálogo de software

1 En Symantec Management Console, en el menú **Administrar**, haga clic en **Catálogo de software**.

2 En la ventana **Catálogo de software**, realice una de las siguientes acciones:

- Para un componente de software indefinido, en el panel **Software recientemente detectado/definido**, selecciónelo y después haga clic en el símbolo **Edit**. Si el componente de software indefinido no está en la lista, haga clic en **Show all software** en la parte inferior de la lista.
- Para un componente de software definido, localice el producto de software con el que se asocia el componente de software en la lista **Productos de software administrados** o **Software no administrado**. A continuación, haga clic en el signo **Más** que precede al producto de software y haga clic en el vínculo para el componente de software que aparece debajo del producto de software.

3 En la página del recurso de software, en la ficha **Paquete**, en el panel **Paquetes**, haga clic en el paquete cuyos puntos de distribución desea actualizar.

4 Haga clic en **Acciones > Actualizar puntos de distribución**.

Para actualizar los puntos de distribución de paquetes para un paquete al que se accede desde el menú Configuración

1 En Symantec Management Console, en el menú **Configuración**, haga clic en **Todas las configuraciones**.

2 En el panel izquierdo, seleccione el paquete cuyos puntos de distribución desea actualizar.

3 En la página **Paquete**, en la parte inferior de la página, haga clic en **Actualizar puntos de distribución**.

Habilitación del acceso a un paquete en una ubicación UNC de origen

Symantec Management Agent usa la Credencial de conectividad del agente (ACC) para conectarse a IIS en Notification Server para descargar los paquetes de UNC con HTTP. IIS se autentica con el origen de UNC mediante las credenciales del punto de distribución (DPC). Symantec Management Agent usa la ACC para conectarse a orígenes de descarga. Asegúrese de que la ACC tenga acceso de lectura cuando Symantec Management Agent realiza descargas directamente del origen del paquete de UNC.

No se usa DPC si Symantec Management Agent descarga un paquete de un servidor de paquetes. El servidor de paquetes aplica cualquier acceso anónimo o la ACC a los archivos de paquete descargados.

Para habilitar el acceso a un paquete en una ubicación UNC de origen

1 Especifique las credenciales de punto de distribución de paquetes que desee usar.

Se especifican estas credenciales en la ficha **Credenciales del punto de distribución** de la página **Valores de configuración de Notification Server**. Se recomienda seleccionar **Usar credencial de conectividad del agente** cuando especifica las credenciales del punto de distribución del paquete. Esta opción garantiza que solamente una credencial (la ACC) sea necesaria en ubicaciones de orígenes UNC de paquetes.

Ver "Configuración de las credenciales del punto de distribución" en la página 75.

2 Asigne acceso de lectura a estas credenciales en la carpeta UNC de origen.

Cómo administrar programas del paquete

Un paquete puede tener más de un programa. Es posible administrar los programas en un paquete para adaptarse a sus requisitos. Es posible cambiar los detalles del programa, agregar nuevos programas al paquete y quitar cualquier programa que ya no necesite.

Ver "Cómo cambiar la configuración de un paquete" en la página 370.

Para visualizar los detalles de un programa del paquete

1 En Symantec Management Console, en el menú **Configuración**, haga clic en **Todas las configuraciones**.

2 En el panel izquierdo, seleccione el paquete que desee modificar.

3 En la página Paquete, en la ficha **Programas**, seleccione el programa que desee ver.

Para crear un nuevo programa del paquete

1 En Symantec Management Console, en el menú **Configuración**, haga clic en **Todas las configuraciones**.

2 En el panel izquierdo, seleccione el paquete que desee modificar.

3 En la página Paquete, en la ficha **Programas**, haga clic en **Nuevo**.

4 Especifique los detalles del programa en los campos apropiados.

5 Haga clic en **Aplicar**.

Para quitar un programa de un paquete

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Todas las configuraciones**.
2. En el panel izquierdo, seleccione el paquete que desee modificar.
3. En la página Paquete, en la ficha **Programas**, seleccione el programa que desee quitar y después haga clic en **Eliminar**.
4. Haga clic en **Aplicar**.

Capítulo 25

Uso de directivas

En este capítulo se incluyen los temas siguientes:

- Acerca de las políticas de Symantec Management Platform
- Acerca de las políticas basadas en el usuario
- Cómo administrar las políticas de Symantec Management Platform
- Aplicar una política usando arrastrar y soltar
- Especificación de destinos de una política o tarea
- Modificación de un destino de recursos
- Cómo generar un destino de recursos
- Cómo seleccionar un destino de recursos existente
- Cómo guardar un destino de recursos con nombre
- Cómo especificar reglas de filtro para los destinos de recursos
- Cómo seleccionar los destinos de recursos con nombre
- Cómo especificar una programación de política
- Configurar las políticas de instalación, actualización y desinstalación del agente o complemento
- Acerca de las políticas de automatización
- Componentes principales de las políticas de automatización
- Administración de políticas de automatización
- Creación o modificación de políticas de automatización programadas
- Creación o modificación de políticas de automatización basadas en mensajes

- Creación y modificación de tareas de políticas de automatización

Acerca de las políticas de Symantec Management Platform

Una política de Symantec Management Platform es un conjunto de reglas que se aplican a un recurso o a un conjunto de recursos (conocidos como el destino de la política). Una política se puede evaluar sobre la base de una programación o de datos entrantes. Cuando se evalúa una política, se aplica la acción apropiada. Esta acción incluye típicamente la ejecución de tareas en los recursos de destino para garantizar que todos cumplan con la política.

Tabla 25-1 Tipos comunes de políticas de Symantec Management Platform

Tipo de política	Descripción
Agente	Especifica los valores de configuración de Symantec Management Agent en los equipos cliente. Ver "Cómo configurar Symantec Management Agent" en la página 276.
Automatización	Especifica acciones automatizadas para realizar en equipos cliente o en el equipo con Notification Server. Estas políticas son dinámicas. Señalan a los equipos apropiados cuando se activa la política y realizan la acción que sea necesaria sobre la base del estado actual de cada equipo de destino. Los destinos de la política de automatización se pueden basar en los resultados de un informe o una consulta, en lugar de filtros y destinos de recursos como con otros tipos de políticas. Ver "Acerca de las políticas de automatización" en la página 391.
Usuario	Especifica la configuración que se aplica a usuarios determinados. Esta configuración se aplica a los equipos donde los usuarios iniciaron sesión. Ver "Acerca de las políticas basadas en el usuario" en la página 377.
Solución	Las soluciones pueden suministrar sus propias políticas que señalan a los equipos o los usuarios de esas soluciones.

Acerca de las políticas basadas en el usuario

Las políticas basadas en el usuario se pueden aplicar a usuarios o grupos de usuarios específicos. También podrían aplicarse a equipos específicos (pero no necesariamente).

Ver "Acerca de las políticas de Symantec Management Platform" en la página 376.

Por ejemplo, algunas organizaciones tienen una gran cantidad de grupos de seguridad de Active Directory y desean asignar políticas mediante dichos grupos de seguridad. Los grupos de seguridad contienen equipos o usuarios administrados que se importan en la CMDB. El uso de políticas basadas en el usuario permite que el administrador maneje los equipos con la infraestructura de Active Directory existente. Se admiten los grupos de trabajo y los usuarios locales.

Las políticas basadas en el usuario solamente se aplican cuando el usuario inicia sesión en un equipo administrado. Dichas políticas se aplican solamente al usuario que haya iniciado sesión en la sesión de consola. Cada vez que un usuario inicie sesión en un equipo administrado, Symantec Management Agent busca las políticas basadas en el usuario que se aplican a dicho usuario. Las políticas se almacenan en la memoria caché del equipo durante una semana. Symantec Management Agent también realiza solicitudes de configuración regulares para cualquier política activa que utilice el SID del usuario que ha iniciado sesión, además del GUID del equipo administrado, a fin de recibir tanto las políticas basadas en el usuario como las basadas en el equipo. El agente efectúa esta solicitud la primera vez que el usuario inicia sesión en un equipo administrado. El agente repite la solicitud cada vez que realiza una solicitud de configuración normal.

Nota: Los usuarios que inician sesión en los equipos administrados a través de servicios de terminal no reciben las políticas que están dirigidas a ellos. Todos los usuarios ven las políticas que se aplican al usuario que haya iniciado sesión en la sesión de consola.

Quizá desee excluir algunos equipos o usuarios de las políticas basadas en el usuario. Por ejemplo, un equipo administrado que comparten muchos usuarios o un administrador que puede iniciar sesión en varios equipos diferentes diariamente. Si dicho equipo o usuario es el destino de una política basada en el usuario, los cambios frecuentes activados por las políticas podrían imponer una sobrecarga considerable en los equipos afectados.

Es posible crear una lista de equipos en los que no se aplican las políticas basadas en el usuario. Es posible crear una lista de usuarios a quienes no deben destinarse las políticas basadas en el usuario. Puede cambiar dichas listas como exclusiones en los filtros apropiados.

Ver "Acerca de los filtros de recursos" en la página 353.

Ver "Creación o modificación de un filtro" en la página 354.

Cómo administrar las políticas de Symantec Management Platform

La vista Políticas recopila todas las políticas disponibles en una única estructura de carpeta. Esta estructura estándar permite fácilmente acceder a las políticas que desee ver o modificar.

Ver "Acerca de las políticas de Symantec Management Platform" en la página 376.

Ver "Acerca de las políticas de automatización" en la página 391.

Para administrar las políticas

1. En Symantec Management Console, en el menú **Administrar**, haga clic en **Políticas**.
2. En el panel izquierdo, bajo la carpeta Políticas, seleccione la política o grupo de políticas que desee administrar.

Aplicar una política usando arrastrar y soltar

En la vista **Políticas**, se puede buscar, ver y aplicar políticas. Esta vista mejorada tiene un campo de búsqueda, que le permite encontrar rápidamente las políticas con las cuales desee trabajar. Es posible buscar por el nombre de política o el tipo de políticas.

Ver "Acerca de la vista Políticas " en la página 44.

Es posible poner en marcha las políticas arrastrándolas y soltándolas en uno o más equipos. Además, se puede usar la opción **Aplicar rápidamente en** para seleccionar el destino de una política sin examinar niveles inferiores manualmente.

Ver "Especificación de destinos de una política o tarea" en la página 379.

Nota: Es necesario tener uno de los siguientes conjuntos de aplicaciones o soluciones instalados para realizar esta tarea: Deployment Solution (producto independiente), IT Management Suite, Server Management Suite o Client Management Suite.

Para aplicar una política usando arrastrar y soltar

1. En Symantec Management Console, en el menú **Administrar**, haga clic en **Políticas**.
2. En el panel de navegación, haga clic en la política que desee ejecutar y arrástrela a la derecha para iniciar la operación de arrastrar y soltar.

   Los resultados de la búsqueda informática más reciente aparecen en el panel de lista. Si filtró la búsqueda informática más actual, la lista muestra los resultados de la búsqueda filtrada.

   Ver "Buscar un equipo y guardar la búsqueda como filtro" en la página 39.
3. Para seleccionar los equipos en los cuales desee ejecutar la política, realice una de las siguientes opciones:
   - Para ejecutar la política en todos los equipos enumerados, suéltela sobre el icono del título en el panel de lista.
   - Para ejecutar la política en un equipo específico, suéltela sobre el equipo en la lista.
   - Para ejecutar la política en una búsqueda guardada, vista organizativa o grupo organizativo, arrástrela a la hoja **Equipos** y a continuación suéltela sobre una búsqueda guardada, una vista organizativa o un grupo organizativo
4. En el cuadro de diálogo **Aplicar la política**, haga clic en **Aceptar**.

Especificación de destinos de una política o tarea

Debe especificar uno o más destinos de una política o tarea. Un destino define el equipo, los usuarios y los recursos en los cuales se aplique la política o tarea. La política o tarea podría tener varios destinos.

Es posible aplicar los siguientes tipos de destinos a una política o tarea:

Destinos de recursos generados automáticamente	A estos destinos no se les ha dado un nombre y no se han guardado explícitamente. Los destinos generados automáticamente se usan solamente por la política o la tarea en las cuales se crean. Es posible editar estos destinos cuando se modifica la política o la tarea, pero no se puede aplicarlos a ninguna otra política o tarea.

Destinos de recursos con nombre	Estos destinos se han guardado explícitamente como destinos de recursos con nombre. Los destinos con nombre se pueden aplicar a cualquier cantidad de tareas y políticas, y pueden ser modificados por cualquier usuario que tenga los permisos apropiados. Ver "Cómo guardar un destino de recursos con nombre" en la página 383.

Los destinos no se muestran como elementos en ningún lugar de Symantec Management Console. Sin embargo, se puede usar la opción **Aplicar rápidamente en** para seleccionar los destinos con nombre existentes y aplicarlos a una política o a una tarea. Es posible ver además la lista de destinos con nombre disponibles en el cuadro de diálogo **Guardar como** cuando se crea o modifica un destino con nombre.

Ver "Acerca de los destinos de recursos" en la página 366.

Para especificar el destino de una política o una tarea

1. En Symantec Management Console, en el menú **Administrar**, haga clic en **Políticas**.
2. En el panel izquierdo, bajo la carpeta Políticas, seleccione la política o grupo de políticas que desee administrar.
3. En la página *Nombre de política* o *Nombre de tarea*, en **Aplicar a/Cumplimiento**, haga clic en **Aplicar a** y después haga clic en una de las siguientes opciones:

Aplicar rápidamente en	1 En el cuadro de diálogo **Aplicar rápidamente en**, en la lista desplegable, seleccione el destino con nombre, el grupo organizativo o el filtro correspondientes. 2 (Opcional) Escriba las primeras tres letras del elemento que desee. Las opciones en la lista se limitan a aquellas que coincidan con las letras escritas. 3 Haga clic en **Aplicar**.
Equipos	En la ventana **Seleccionar equipos**, seleccione los equipos que desee. Ver "Cómo generar un destino de recursos" en la página 382.
Usuarios	En la ventana **Seleccionar usuarios**, seleccione los usuarios que desee. Ver "Cómo generar un destino de recursos" en la página 382.

Recursos	En la ventana **Seleccionar recursos**, seleccione los recursos que desee. Ver "Cómo generar un destino de recursos" en la página 382.

Tenga en cuenta que algunas opciones puede no estar disponible para todas las políticas.

Cada selección se añade a la lista de destinos en la cuadrícula **Aplicar a**.

Repita este paso para agregar todos los destinos que desee.

4 (Opcional) En la lista desplegable **View**, haga clic en la opción apropiada: **Equipos y usuarios**, **Applied by** o **Ejecuciones de tareas**.

La lista muestra solamente los elementos que se hayan seleccionado explícitamente. Por ejemplo, si visualiza equipos, solamente verá los que haya seleccionado en la ventana **Seleccionar equipos**. No podrá ver ningún equipo adicional que esté contenido en los destinos que haya seleccionado en el cuadro de diálogo **Aplicar rápidamente en**.

5 Si desea modificar un destino o eliminarlo de la lista, selecciónelo en la cuadrícula **Se aplica a/Cumplimiento** y, a continuación, haga clic en **Editar** o **Eliminar**, la que sea apropiada.

Ver "Modificación de un destino de recursos" en la página 381.

6 Haga clic en **Guardar cambios**.

Modificación de un destino de recursos

Cuando se modifica una política o una tarea, se puede modificar cualquier destino generado automáticamente que lo contenga y cualquier destino de recursos con nombre para el que se tenga acceso.

Ver "Especificación de destinos de una política o tarea" en la página 379.

Ver "Cómo administrar las políticas de Symantec Management Platform" en la página 378.

Para modificar a un destino de recursos

1 En Symantec Management Console, en el menú **Administrar**, haga clic en **Políticas**.

2 En el panel izquierdo, bajo la carpeta Políticas, seleccione la política o grupo de políticas que desee administrar.

3 En la página *Nombre de política* o la página *Nombre de tarea*, en el panel **Se aplica a/Cumplimiento**, en la lista desplegable **View**, haga clic en **Equipos y Usuarios**.

4 En la cuadrícula **Se aplica a/Cumplimiento**, seleccione el destino que desea modificar.

5 Haga clic en **Editar**.

6 En la ventana **Editar grupo seleccionado**, realice los cambios necesarios al destino.

Ver "Cómo generar un destino de recursos" en la página 382.

Cómo generar un destino de recursos

Las ventanas **Seleccionar equipos**, **Seleccionar usuarios** y **Seleccionar recursos** permiten seleccionar los elementos que desee incluir en un destino de recursos. La ventana **Editar grupo seleccionado** permite cambiar la selección para un destino de recursos existente.

Ver "Especificación de destinos de una política o tarea" en la página 379.

Para generar un destino de recursos

1 En Symantec Management Console, en el menú **Administrar**, haga clic en **Políticas**.

2 En el panel izquierdo, bajo la carpeta Políticas, seleccione la política o grupo de políticas que desee administrar.

3 En la página *Nombre de política* o página *Nombre de tarea*, en el panel **Se aplica a/Cumplimiento**, haga doble clic en el recurso que usted quiere administrar.

4 Si usted quiere basar el recurso de destino en un destino denominado existente, en el cuadro de diálogo **Agregar destino**, haga clic en **Open** y luego, en la ventana **Open**, seleccione el destino apropiado.

Ver "Cómo seleccionar un destino de recursos existente" en la página 383.

5 En **Reglas de filtrado**, especifique las reglas con las que desee filtrar los equipos, los usuarios o los recursos disponibles.

Ver "Cómo especificar reglas de filtro para los destinos de recursos" en la página 384.

6 Si desea guardar el destino de recursos como un destino con nombre, haga clic en **Guardar como**.

Ver "Cómo guardar un destino de recursos con nombre" en la página 383.

7 Cuando la lista **Elementos que coinciden actualmente con las reglas** muestre los elementos que desee, haga clic en **Aceptar**.

Se añade el destino de recursos especificado a la política o a la tarea. Si el destino se generó automáticamente (que no se ha guardado como destino con nombre), se le otorga un nombre predeterminado que se basa en los nombres de los grupos organizativos y los filtros que usa.

Cómo seleccionar un destino de recursos existente

El cuadro de diálogo **Abrir** permite seleccionar un destino de recursos con nombre a existente o grupo con nombre de destinos de recursos (que en sí es un destino de recursos). Si se accede a este cuadro de diálogo desde el Generador de destinos de recursos (por lo general, llamada ventana **Seleccionar recursos**) o desde el Selector de destinos de recursos (por lo general, llamada ventana **Seleccionar destino de recursos** o **Seleccionar un grupo**), el destino o grupo de destinos que se selecciona aquí reemplaza la selección actual en la ventana. Si se accede a este cuadro de diálogo desde la ventana del selector de recursos (**Seleccionar equipos** o **Seleccionar recursos**), la pertenencia del destino se añade a la selección actual en la ventana.

Ver "Especificación de destinos de una política o tarea" en la página 379.

Ver "Cómo guardar un destino de recursos con nombre" en la página 383.

Para seleccionar un destino de recursos existente

1 En la ventana **Seleccionar equipos/recursos**, la ventana **Seleccionar un grupo** o la ventana **Editar el grupo seleccionado**, haga clic en **Abrir**.

2 En el cuadro de diálogo **Abrir**, en la lista de destino de recursos o de grupos con nombre, haga clic en el destino o grupo apropiado.

3 Haga clic en **Aceptar**.

Cómo guardar un destino de recursos con nombre

Si desea usar un destino de recursos en varias tareas y políticas o hacer que esté disponible para otros usuarios, se puede guardar el destino como un destino de recursos con nombre. Los destinos con nombre pueden aplicarse a cualquier cantidad de tareas y políticas. Cualquier usuario que tenga los permisos apropiados puede acceder o modificar cualquier destino con nombre que se cree. Es posible

también guardar los grupos con nombre de destino de recursos cuando es apropiado, por ejemplo, para la inclusión en reglas de replicación.

Ver "Especificación de destinos de una política o tarea" en la página 379.

Ver "Cómo seleccionar los destinos de recursos con nombre" en la página 386.

Ver "Cómo seleccionar un destino de recursos existente" en la página 383.

Si se accede a la ventana **Guardar como** desde el Selector de destino de recursos (por lo general, llamada ventana **Seleccionar destino de recursos** o **Seleccionar un grupo**), puede guardar los destinos de recursos seleccionados como un grupo con nombre de los destinos de recursos. Si accede a la ventana **Guardar como** desde el Generador de destinos de recursos (por lo general, llamada ventana **Seleccionar equipos** o **Seleccionar recursos**), puede guardar los recursos seleccionados (que se pueden especificar explícitamente o seleccionar dinámicamente con una consulta) como destino de recursos con nombre.

Para guardar un destino de recursos con nombre

1. En la ventana **Seleccionar equipos/recursos**, la ventana **Seleccionar un grupo** o la ventana **Editar el grupo seleccionado**, haga clic en **Guardar como**.
2. En el cuadro de diálogo **Guardar como**, realice una de las siguientes acciones:

Para crear un nuevo destino o grupo	En el cuadro **Nombre**, escriba el nombre apropiado para el destino o el grupo.
Para sobrescribir un destino o grupo existente	En la lista de destinos o grupos con nombre, haga clic en el nombre apropiado. Solamente puede seleccionar los destinos o los grupos para los cuales tiene acceso de escritura. No podrá seleccionar los destinos o grupos de solo lectura.

3. Haga clic en **Aceptar**.

Cómo especificar reglas de filtro para los destinos de recursos

Las reglas de filtro le permiten filtrar equipos, usuarios y recursos para identificar los elementos que desea seleccionar. Las reglas se aplican de acuerdo con el orden en el cual se han instalado, de manera que cualquier elemento que haya sido excluido se lo puede incluir nuevamente mediante una norma posterior. La lista **Elementos que coinciden actualmente con reglas** muestra aquellos

elementos que las reglas específicas han seleccionado. La lista se actualiza de forma automática a medida que agrega y modifica las reglas de filtro.

Ver "Especificación de destinos de una política o tarea" en la página 379.

Para especificar una norma de filtro

1 En la ventana **Seleccionar elementos**, en **Reglas de filtrado**, haga clic en **Agregar regla**.

2 En la primera lista desplegable, haga clic en una operación apropiada:

Excluir elementos de	Excluye los elementos que están en el filtro especificado o en un grupo organizativo como también aquellos recursos de la lista de elementos.
Excluir elementos que no están en	Excluye los elementos que no están en el filtro especificado o en un grupo organizativo como también aquellos recursos seleccionados de la lista de elementos.

3 En la segunda lista desplegable, haga clic en una opción apropiada:

Filtro	Aplicar la operación a un filtro específico.
Grupo	Aplicar la operación a un grupo organizativo específico.
Lista de elementos	Aplicar la operación a equipos, usuarios o recursos específicos.

4 En la tercera lista desplegable, seleccione un elemento apropiado:

Para seleccionar un filtro o grupo	Escriba las primeras letras del filtro o del grupo organizativo que desee. Las opciones en la lista se limitan a aquellas que coincidan con las letras escritas.
Para seleccionar elementos específicos	Haga clic en la elipse (**...**) y, a continuación, en la ventana **Seleccionar elemento**, seleccione los elementos apropiados.

Para administrar la lista de reglas de filtro

1 Si desea subir o bajar una regla en la lista de reglas de filtro, haga clic en las flechas ascendentes o descendentes.

2 Si desea quitar una norma de filtrado de la lista, haga clic en **Eliminar**.

Cómo seleccionar los destinos de recursos con nombre

La ventana **Seleccionar destino de recurso** o **Seleccionar un grupo** permite seleccionar los destinos de recursos con nombre que desea usar. El panel izquierdo visualiza la lista de destinos de recursos disponibles y el panel derecho visualiza la lista de destinos de recursos seleccionados.

Ver "Especificación de destinos de una política o tarea" en la página 379.

Es posible filtrar los destinos de recursos seleccionados en el panel izquierdo por vista organizativa o por un grupo organizativo determinado. El filtro restringe la pertenencia de los destinos seleccionados a los recursos que están contenidos en la vista organizativa o de grupo especificada. Es posible también crear los nuevos destinos de recursos con nombre.

Es necesario agregar los destinos de recursos que desee seleccionar a la lista de destinos de recursos en el panel derecho. Es posible también guardar los destinos de recursos seleccionados como un grupo nombrado de destinos de recursos.

Para seleccionar destinos de recursos con nombre

1. (Opcional) Si desea filtrar la pertenencia de los destinos de recursos seleccionados por una vista organizativa o de grupo determinada, en la lista desplegable **Grupo**, seleccione la vista organizativa o de grupo.
2. (Opcional) Si desea crear un nuevo destino de recursos con nombre, haga clic en **Generar destino**.

   Ver "Cómo generar un destino de recursos" en la página 382.
3. En el panel izquierdo, seleccione los destinos de recursos que desee y, luego, haga clic en **>** para agregarlos a la lista seleccionada de destinos de recursos en el panel derecho.
4. (Opcional) Si desea seleccionar los destinos de recursos que se contienen en un grupo nombrado existente de destinos de recursos, haga clic en **Abrir** y, a continuación, en el cuadro de diálogo **Abrir**, seleccione el grupo apropiado.

   Ver "Cómo seleccionar un destino de recursos existente" en la página 383.

   Los destinos de recursos en el grupo seleccionado se agregan a la lista en el panel derecho.
5. (Opcional) Si desea quitar cualquier destino de recursos de la lista de destino, seleccione los destinos de recursos apropiados y, luego, haga clic en **<**.

6 (Opcional) Si desea guardar los destinos de recursos en la lista de destinos seleccionada como grupo nombrado para un uso posterior, haga clic en **Guardar como** y, en el cuadro de diálogo **Guardar como**, especifique el nombre apropiado.

Ver "Cómo guardar un destino de recursos con nombre" en la página 383.

7 Haga clic en **Aceptar**.

Cómo especificar una programación de política

Es necesario especificar la hora en que una política se activa configurando las programaciones apropiadas. Puede especificar la cantidad de programaciones que necesite y tener cualquier cantidad de programaciones activas al mismo tiempo.

Ver "Acerca de las políticas de Symantec Management Platform" en la página 376.

Este tema además se aplica a algunas otras programaciones, como la programación de la actualización de pertenencia a recursos. Algunas opciones que se describen aquí pueden no estar disponibles para todas las políticas.

Para especificar una programación de política

1 En la página Políticas, en **Programación**, haga clic en **Agregar programación** y, a continuación, haga clic en una de las siguientes opciones:

Hora programada	1 En el cuadro Inicio, especifique la hora apropiada. 2 Si desea que la programación se repita, haga clic en **No repetir** y, a continuación, en el cuadro de diálogo **Repetir la programación**, especifique la frecuencia apropiada.
Ventana de programación	1 En los cuadros Inicio, Fin y Duración, especifique las horas apropiadas. 2 En la ventana de **Durante**, compruebe cada cuadro y especifique el intervalo apropiado. 3 Si desea que la programación se repita, haga clic en **No repetir** y, a continuación, en el cuadro de diálogo **Repetir la programación**, especifique la frecuencia apropiada.
Cuando el usuario inicie sesión	Se activa la política cuando un usuario inicia sesión en el equipo administrado.
Al iniciar el equipo	Se activa la política cuando el equipo administrado se inicia.

Cada programación se añade a la lista de programaciones de política. Repita este paso para agregar todas las programaciones que desee.

2 En la lista desplegable **Zona horaria**, seleccione la zona horaria apropiada:

Utilizar la hora del agente	La hora se especifica sin la información de la zona horaria y se aplica a la hora local en cada equipo administrado. Las programaciones se ejecutan a diferentes horas según las zonas horarias de los equipos administrados.
Utilizar la hora del servidor	La hora se especifica con la información de la zona horaria, donde el desfase de zona horaria es el de la zona horaria del servidor en el que está definida la política. Las programaciones se ejecutan de forma simultánea independientemente de las zonas horarias y se compensan para el horario de verano. Esta opción asegura que las programaciones estén coordinadas siempre con la hora local especificada en el servidor en el que se crea la política.
Coordinar mediante UTC	La hora se especifica con la información de la zona horaria, donde el desfase de zona horaria es 0. Las programaciones se ejecutan en forma simultánea independientemente de las zonas horarias y no las afecta el horario de verano.

3 Haga clic en **Opciones avanzadas** y, a continuación, en el cuadro de diálogo **Opciones Avanzadas**, realice los cambios apropiados:

Sólo realizar verificación si:	Compruebe las opciones apropiadas: ■ El equipo está conectado a la red ■ El equipo se encuentra disponible a la hora exacta programada ■ Un usuario ha iniciado sesión en el equipo ■ Un usuario no ha iniciado sesión en el equipo

Fechas de inicio o finalización	La fecha de inicio es la fecha en que la política surte efecto. La política debe habilitarse igual que cualquier otra política. Es posible habilitar la política en cualquier momento antes o después de la fecha de inicio. Si desea que la política esté disponible por un periodo de tiempo limitado, configure la fecha de finalización apropiada. La política no está disponible después de esta fecha, independientemente de si está habilitada. La configuración de la fecha de finalización es opcional. Si no se especifica ninguna fecha de finalización, la política está disponible indefinidamente.

4 Haga clic en **Aceptar** para cerrar el cuadro de diálogo Opciones avanzadas.

5 (Opcional) si desea quitar una programación de la lista, selecciónela y, a continuación, haga clic en **Eliminar**.

Configurar las políticas de instalación, actualización y desinstalación del agente o complemento

Es posible configurar la instalación del agente, la actualización del agente y las políticas de desinstalación del agente para satisfacer sus requisitos. Estas políticas usan el mismo paquete del agente, pero cada política usa un programa diferente.

Para configurar las políticas de instalación, actualización y desinstalación del agente o complemento

1 En Symantec Management Console, en el menú **Configuración**, haga clic en **Todas las configuraciones**.

2 En el panel izquierdo, expanda la carpeta apropiada y, luego, seleccione la política que desee configurar.

3 (Opcional) Para activar o desactivar las políticas, en **Instalación del agente**, **Actualización del agente**, o en la página **Desinstalación del agente**, haga clic en el símbolo de estado y, luego, haga clic en **Activar** o **Desactivar**.

4 Realice los cambios adecuados en la configuración:

Nombre de programa	Nombre del programa del paquete del agente que se ejecuta cuando se activa la política. La configuración predeterminada establece el programa que es apropiado para la política y no debe cambiarse. No obstante, si ha agregado un programa nuevo al paquete del agente, quizá desee utilizarlo. Ver "Cómo administrar programas del paquete" en la página 373.
Habilitar un informe prolijo de los eventos de estado	Habilite el envío de tipos de eventos del estado a Notification Server. La configuración de **Captura de evento de Notification Server** en la política de configuración global de Symantec Management Agent tiene precedencia sobre la configuración de **Habilitar un informe detallado**. Los eventos se envían solamente si están habilitados en la política de configuración global de Symantec Management Agent. Ver "Configuración de las opciones de configuración global de agente" en la página 277.
Se aplicó a	Especifique los equipos a los cuales se aplica la política. Puede utilizar los filtros predefinidos que se proporcionan con Notification Server o crear sus propios filtros. Ver "Especificación de destinos de una política o tarea" en la página 379.
Multidifusión de paquetes	Deshabilita la descarga de paquetes a través de la multidifusión. Por lo general, la multidifusión reduce la velocidad de la distribución de los paquetes, de modo que quizá desee desactivarla para instalar revisiones urgentes. Además, en algunos entornos, la multidifusión no funciona. Por ejemplo, es posible que esté deshabilitada en los enrutadores y los conmutadores. La configuración de Multidifusión de paquetes de la política Configuración global de Symantec Management Agent tiene precedencia sobre la configuración que aparece aquí.
Programación	Especifique la programación de la política. Ver "Cómo especificar una programación de política" en la página 387.

Opciones de programación adicionales	Otras opciones de programación son: ■ **Ejecutar una vez lo más pronto posible** ■ **El usuario puede ejecutar** ■ **Notificar al usuario cuando la tarea esté disponible** ■ **Advertir antes de ejecutar**

5 Haga clic en **Guardar cambios**.

Acerca de las políticas de automatización

Las políticas de automatización son conjuntos de reglas definidas por el usuario o por el administrador, las cuales rigen la ejecución de las acciones automatizadas. Algunos ejemplos de acciones automatizadas incluyen: la ejecución de un informe con los parámetros obtenidos de la política, el envío de una alerta al administrador y la ejecución de un comando o de una tarea en los equipos administrados.

Ver "Acerca de las políticas de Symantec Management Platform" en la página 376.

Ver "Administración de políticas de automatización" en la página 393.

Ver "Componentes principales de las políticas de automatización" en la página 392.

Las políticas de automatización se pueden ejecutar en una programación o ser activadas por mensajes de Notification Server. La política determina el momento en que debe empezar una acción y a quién o a qué deben notificarse los resultados. Las políticas de automatización se ejecutan en el equipo con Notification Server, de modo que no tienen nada que ver con la actividad relacionada con el agente en los equipos administrados. No obstante, algunas políticas de automatización podrían ser activadas por mensajes generados por la actividad del agente.

Las políticas de automatización no se aplican a los destinos de recursos, a diferencia de otros tipos de políticas de Notification Server. Constituyen acciones de Notification Server, las cuales se realizan en los equipos administrados apropiados. Algunas acciones, como el envío de mensajes de correo electrónico al administrador, que contengan un informe o un origen de datos, como un archivo HTML, no afectan ningún equipo administrado.

Muchas de las soluciones que funcionan con Notification Server vienen con políticas de automatización. Estas políticas permiten a Notification Server realizar una variedad de acciones cuando ocurren las condiciones definidas. Las políticas de automatización se pueden configurar en un solo proceso que se inicia en un equipo. , las políticas de automatización también se pueden configurar en situaciones complejas, como varios procesos en una gran cantidad de equipos. Cada solución que define las políticas de automatización especifica los propios criterios para el tipo de condiciones que lleven a las acciones iniciadas.

Por ejemplo, Inventory Solution utiliza datos de la CMDB y la medición de aplicaciones utiliza la lista de procesos supervisados. En esta solución, sin embargo, existen conjuntos comunes de acciones que se pueden ejecutar de manera automática.

Componentes principales de las políticas de automatización

Ver "Acerca de las políticas de automatización" en la página 391.

Las políticas de automatización tienen los mismos componentes principales.

Tabla 25-2 Componentes fundamentales de las políticas de automatización

Componente	Descripción
Desencadenador	Inicia la evaluación de una política de automatización. Notification Server proporciona las activaciones siguientes: ■ Programación Cualquier programación de Notification Server, tales como una programación compartida o una programación personalizada específica. No puede utilizar ventanas de mantenimiento (las cuales se definen en equipos administrados) como desencadenantes de políticas de automatización. ■ Mensaje Un mensaje interno de Notification Server. Estos mensajes se envían cuando ocurren eventos de interés. Por ejemplo, un recurso creado, un recurso detectado, un recurso eliminado, un equipo nuevo detectado o el inicio de servicio de Notification Server.

Componente	Descripción
Origen de datos	Proporciona información que utiliza la política de automatización tras haber sido desencadenada. El origen de datos es, generalmente, un informe o consulta que devuelve una lista de equipos junto con información sobre el estado de cada equipo y su configuración actual los cuales son relevantes a la política. El informe o consulta se ejecutan cuando la política se desencadena para asegurar que los datos más recientes son extraídos. El origen de datos define los equipos administrados que han sido afectados por la política y las acciones que se realizan sobre los mismos. Una política de automatización puede extraer también parámetros del origen de datos y utilizarlos como parámetros de entrada para tareas o trabajos. Notification Server ofrece los siguientes orígenes de datos: ■ **Informe** ■ **Consulta SQL sin procesar** Si selecciona esta opción, se necesita el privilegio de **editar SQL directamente** para poder editar la consulta del origen de datos y ver los resultados de la consulta. Ver "Privilegios del sistema" en la página 494. ■ **Consulta de recursos** ■ **Mensaje** ■ **Ninguno(a)** Las soluciones pueden agregar orígenes de datos adicionales.
Regla de evaluación	Evalúa los datos que se encuentran en el origen de datos y determina si una acción necesita realizarse o no. Notification Server ofrece las siguientes reglas de evaluación: ■ Ejecutar cuando haya datos que no estén en blanco ■ Ejecutar para cada registro ■ Procesamiento de mensaje ■ Ejecutar siempre
Acción	Especifica la tarea o trabajo que la política ejecuta. Estas son tareas estándar del servidor o agente. La acción puede incluir parámetros de entrada que provienen del origen de datos.

Administración de políticas de automatización

Puede configurar y administrar las políticas de automatización que tiene disponible en Notification Server. Puede crear políticas nuevas, editar las existentes, activarlas o desactivarlas cuando sea necesario, establecer la seguridad debida en ellas y eliminarlas cuando ya no se necesiten.

Ver "Acerca de las políticas de automatización" en la página 391.

Para administrar políticas de automatización

1. En Symantec Management Console, en el menú **Administrar**, haga clic en **Políticas de automatización**.
2. En la página **Políticas de automatización**, seleccione la ficha apropiada:

Programaciones	Administrar las políticas de automatización que se ejecuten en una programación predefinida.
Mensajes del sistema	Administrar políticas de automatización que se ejecuten cuando se reciba un mensaje de sistema específico.

3 Efectúe uno de los pasos siguientes:

Crear o modificar una política	Ver "Creación o modificación de políticas de automatización programadas" en la página 396. Ver "Creación o modificación de políticas de automatización basadas en mensajes" en la página 398.
Activación y desactivación de políticas	En el panel izquierdo, seleccione la política de automatización que desee activar o desactivar y después haga clic en **Encender** o **Apagar** según corresponda.
Eliminar una política	En el panel izquierdo, seleccione la política de automatización que desee eliminar y, después, haga clic en **Eliminar**. Puede eliminar las políticas de automatización que haya creado. No puede eliminar ninguna política de automatización predeterminada proporcionada con Notification Server.
Establecer la seguridad en una política	En el panel izquierdo, seleccione la política de automatización que desee para configurar la seguridad y después haga clic en **Acciones > Seguridad**. En el Administrador de roles de seguridad, establezca la seguridad apropiada.
Realizar otras acciones en una política	En el panel izquierdo, seleccione la política de automatización en la que desee ejecutar la acción y, a continuación, haga clic en **Acciones** y en la opción correspondiente. Las acciones disponibles son las mismas que las del menú contextual.
Probar una política	En el panel izquierdo, seleccione la política de automatización que desee probar y, a continuación, en el panel derecho, haga clic en **Probar política de automatización**. Utilice la prueba de políticas de automatización para verificar que todos los componentes de la política sean coherentes y que los parámetros de entrada se hayan asignado de forma correcta. La prueba ejecuta la política y los resultados de la acción se muestran en el registro Trabajo o tarea.

Creación o modificación de políticas de automatización programadas

Las políticas de automatización pueden utilizar cualquier programación de Notification Server, tal como una programación compartida o una programación personalizada especificada. Las ventanas de mantenimiento (las cuales se definen en los equipos administrados) no se pueden utilizar para programar políticas de automatización. Cuando se desencadena una política de automatización, las acciones correspondientes se ejecutan de inmediato. No puede programar una política de automatización para que se ejecute a una hora posterior después de que se haya activado.

Ver "Acerca de las políticas de automatización" en la página 391.

Ver "Administración de políticas de automatización" en la página 393.

Nota: Este tema cubre las opciones predeterminadas que se suministran con Notification Server. Las soluciones podrían ampliar dichas opciones o agregar nuevas. Para más información, consulte la documentación de la solución correspondiente.

Para crear o modificar una política de automatización programada

1. En Symantec Management Console, en el menú **Administrar**, haga clic en **Políticas de automatización**.
2. En la página **Políticas de automatización**, en la ficha **Programaciones**, realice una de las siguiente acciones:

Para crear una política nueva	1 Haga clic en **Nueva política**. 2 En el cuadro de diálogo **Nombre de la política de automatización**, escriba el nuevo nombre de política y después haga clic en **Aceptar**.
Para modificar una política existente	En el panel izquierdo, seleccione la política apropiada.

3. (Opcional) En el panel derecho, para editar el nombre y la descripción de la política, haga clic en los campos correspondientes y escriba los nuevos detalles.

4 En la lista desplegable **Programación**, seleccione la programación que desea usar.

En la fecha/hora	Especifique la fecha, la hora y la repetición de la programación en los campos correspondientes.
Programación compartida	En la lista desplegable **Seleccionar programación compartida**, seleccione la programación apropiada. Ver "Cómo administrar programaciones compartidas" en la página 122.

5 En el panel **Detalles**, en **Origen de datos**, especifique el origen de datos para usar.

Ver "Especificación del origen de datos de políticas de automatización" en la página 401.

6 En **Condiciones**, en la lista desplegable **Regla de evaluación**, seleccione la regla apropiada de evaluación:

Ejecutar cuando haya datos que no estén en blanco	Trata la tabla de origen de datos como una sola unidad. Cuando se activa la política, la acción se ejecuta solamente si la tabla contiene una o más filas y se ejecuta solo una vez. Debe utilizar esta opción si el origen de datos contiene información en un archivo HTML en lugar de en una tabla. Esta opción permite dirigirse a todo lo que haya en una sola columna, tal como una lista de GUID. No puede establecer parámetros dinámicos para distinguir los equipos de destino. Si desea hacerlo, debe utilizar la ejecución para cada opción de registro.
Ejecutar para cada registro	Evalúa la tabla de origen de datos fila por fila, lo cual permite utilizar campos por fila como parámetros dinámicos para las opciones especificadas. La acción se ejecuta una vez por cada fila.
Ejecutar siempre	Ejecuta las acciones especificadas sin utilizar un origen de datos. Esta opción está disponible solamente cuando no se especifica un origen de datos.

7 En **Acciones**, especifique la tarea o el trabajo que desea ejecutar y configure cualquier parámetro de entrada necesario.

Ver "Especificación de una acción de política de automatización" en la página 402.

8 Haga clic en **Aplicar** para guardar la configuración de políticas.

9 (Opcional) Si desea asegurarse de que todos los componentes de la política sean coherentes y de que los parámetros de entrada se asignen correctamente, haga clic en **Probar política de automatización**.

La prueba consiste solamente en una verificación interna y no afecta ningún recurso.

Creación o modificación de políticas de automatización basadas en mensajes

Las políticas de automatización pueden utilizar un mensaje interno de Notification Server como un desencadenante. Los mensajes que están disponibles para este propósito se encuentran predefinidos. Estos mensajes corresponden a eventos de Notification Server tales como recursos que han sido detectados, creados o eliminados como también equipos nuevos que han sido detectados o servicios de Notification Server que han sido iniciados. Las soluciones pueden hacer que los mensajes específicos de soluciones adicionales se encuentren disponibles. Cuando se desencadena una política de automatización, las acciones correspondientes se ejecutan de inmediato. No puede configurar una política de automatización para que se ejecute más tarde después de haber sido desencadenada.

Ver "Acerca de las políticas de automatización" en la página 391.

Ver "Administración de políticas de automatización" en la página 393.

Nota: Este tema cubre las opciones predeterminadas que se proporcionan con Symantec Management Platform. Las soluciones podrían ampliar dichas opciones o agregar nuevas. Para más información, consulte la documentación de la solución correspondiente.

Para crear o modificar una política de automatización basada en un mensaje

1 En Symantec Management Console, en el menú **Administrar**, haga clic en **Políticas de automatización**.

2 En la página **Políticas de automatización**, en la ficha **Mensajes del sistema**, realice una de las siguientes acciones:

Para crear una política nueva	1 Haga clic en **Nueva política**. 2 En el cuadro de diálogo **Nombre de la política de automatización**, escriba el nuevo nombre de política y después haga clic en **Aceptar**.
Para modificar una política existente	En el panel izquierdo, seleccione la política apropiada.

3 (Opcional) En el panel derecho, para editar el nombre y la descripción de la política, haga clic en los campos correspondientes y escriba los nuevos detalles.

4 En la lista desplegable **Mensaje de NS**, seleccione el mensaje que desea usar.

5 En el panel **Detalles**, en **Origen de datos**, especifique el origen de datos para usar.

Ver "Especificación del origen de datos de políticas de automatización" en la página 401.

6 En **Condiciones**, en la lista desplegable **Regla de evaluación**, seleccione la regla apropiada de evaluación:

Ejecutar cuando haya datos que no estén en blanco	Trata la tabla de origen de datos como una sola unidad. Cuando se activa la política, la acción se ejecuta solamente si la tabla contiene una o más filas y se ejecuta solo una vez. Debe utilizar esta opción si el origen de datos contiene información en un archivo HTML en lugar de en una tabla. Esta opción permite dirigirse a todo lo que haya en una sola columna, tal como una lista de GUID. No puede establecer parámetros dinámicos para distinguir los equipos de destino. Si desea hacerlo, debe utilizar la ejecución para cada opción de registro.
Ejecutar para cada registro	Evalúa la tabla de origen de datos fila por fila, lo cual permite utilizar campos por fila como parámetros dinámicos para las opciones especificadas. La acción se ejecuta una vez por cada fila.
Procesamiento de mensaje	Evalúa el texto del mensaje de origen de datos y utiliza los parámetros apropiados en las acciones específicas. Esta opción está disponible solamente cuando se utiliza un origen de datos del mensaje.
Ejecutar siempre	Ejecuta las acciones especificadas sin utilizar un origen de datos. Esta opción está disponible solamente cuando no se especifica un origen de datos.

7 En **Acciones**, especifique la tarea o el trabajo que desea ejecutar y configure cualquier parámetro de entrada necesario.

Ver "Especificación de una acción de política de automatización" en la página 402.

8 Haga clic en **Guardar cambios** para guardar la política.

9 (Opcional) Si desea asegurarse de que todos los componentes de la política sean coherentes y de que los parámetros de entrada se asignen correctamente, haga clic en **Probar política de automatización**.

La prueba consiste solamente en una verificación interna y no afecta ningún recurso.

Especificación del origen de datos de políticas de automatización

El origen de datos de políticas de automatización determina qué equipos se elegirán y qué acciones se realizarán en ellos. Una política de automatización puede extraer parámetros del origen de datos y utilizarlos como parámetros de entrada para tareas o trabajos.

Ver "Creación o modificación de políticas de automatización programadas" en la página 396.

Ver "Creación o modificación de políticas de automatización basadas en mensajes" en la página 398.

Puede utilizar orígenes de datos externos, como informes y mensajes, o también una consulta para extraer datos de la CMDB. Un origen de datos externo, como un informe, puede ser utilizado por varias políticas de automatización. Sea cuidadoso al utilizar informes, ya que se pueden modificar posteriormente, y los parámetros sobre los cuales dependen algunas acciones pueden ser modificados o eliminados. Si una acción no puede determinar un parámetro requerido de un informe de origen de datos, tal acción utiliza el valor predeterminado que ha sido establecido en la política de automatización.

Ver "Creación y modificación de informes personalizados de Notification Server" en la página 452.

Las consultas SQL y de recurso se integran en la definición de la política de automatización. No puede compartir consultas entre políticas de automatización y tampoco acceder directamente a las consultas (también conocidas como orígenes de datos) que son componentes de los informes. Si desea utilizar una consulta de informe, puede copiar la consulta SQL del informe y pegarla en la política de automatización.

Una política de automatización que no define un destino para su acción no precisa un origen de datos. Por ejemplo, una política que envía un mensaje al administrador o realiza una acción en el equipo con Notification Server

Para especificar el origen de datos de políticas de automatización

1. En Symantec Management Console, en el menú **Administrar**, haga clic en **Políticas de automatización**.
2. En la página **Políticas de automatización**, en la ficha **Mensajes del sistema**, seleccione una política de automatización existente o cree una nueva.
3. En el panel derecho de **Detalles**, en **Origen de datos**, en la lista desplegable **Origen de datos**, seleccione la opción apropiada:

Informe	Utilice los resultados de un informe. 1 En el campo Informe, haga clic en **Nombre del informe**. 2 En la ventana **Seleccionar informe**, seleccione el informe apropiado y después haga clic en **Aceptar**.
Consulta SQL sin procesar	Utilice los resultados de una consulta SQL. 1 Haga clic en **Editar consulta**. 2 En la ventana **Origen de datos**, especifique la consulta SQL que desee usar y después haga clic en **Aceptar**. Ver "Cómo definir una consulta SQL para un filtro" en la página 360. Si desea volver a utilizar una consulta de un filtro o informe existente, puede copiar el contenido de la ficha Consulta resuelta del filtro apropiado o consulta de informe. Luego, puede pegarla en la ficha **Consulta resuelta** de la ventana **Origen de datos**. A continuación, puede modificar la consulta SQL como sea necesario. Tenga en cuenta que la consulta de la ficha **Consulta resuelta** tiene los parámetros reemplazados por los valores de prueba específicos.
Consulta de recursos	Utilice los resultados de una consulta de recursos. 1 Haga clic en **Editar consulta**. 2 En la ventana **Origen de datos**, especifique la consulta de recursos que desee usar y después haga clic en **Aceptar**. Ver "Cómo definir una consulta de recursos para un filtro" en la página 358.
Mensaje	Utilice la información que se encuentra en el mensaje que activó la política.
Ninguno(a)	No se precisa origen de datos. La política de automatización no necesita definir un destino para su acción.

Especificación de una acción de política de automatización

Las acciones de la política de automatización son trabajos y tareas. Symantec Management Platform suministra un conjunto de tareas que se puedan usar y las soluciones pueden agregar más. Es posible crear sus propias tareas y ampliar las opciones para adaptarse a sus requisitos. Si su Symantec Management Platform

forma parte de una jerarquía, más tareas y trabajos pueden reproducirse del Symantec Management Platform principal.

Ver "Creación o modificación de políticas de automatización programadas" en la página 396.

Ver "Creación o modificación de políticas de automatización basadas en mensajes" en la página 398.

Una política de automatización puede contener solamente una acción, que puede ser una tarea o un trabajo, que se aplica a todos los equipos a los que señala la política. Si desea incluir varias tareas, debe incluirlas en un trabajo adecuado. Alternativamente, debe crear varias políticas de automatización con las activaciones, los orígenes de datos y las acciones apropiados.

Advertencia: Varias políticas de automatización pueden compartir un trabajo o una tarea. Cuando modifica una tarea que desea usar en una política de automatización, los cambios podrían afectar a muchas otras políticas. Es posible preferir clonar la tarea relevante y usar la copia modificada en la política.

Las tareas pueden contener parámetros de entrada estáticos y dinámicos. Los parámetros dinámicos se configuran con los valores extraídos del origen de datos cuando se activa la política. Los parámetros estáticos tienen valores configurados en la tarea, de modo que son iguales cada vez que se ejecuta la tarea.

Las acciones de error o los códigos de retorno no pueden ser configurados en una política de automatización, de forma que si cualquiera es necesario, se los debe configurar en la tarea.

Para especificar la acción de la política de automatización

1. En Symantec Management Console, en el menú **Administrar**, haga clic en **Políticas de automatización**.
2. En la página **Políticas de automatización**, en la ficha **Mensajes del sistema**, seleccione una política de automatización existente o cree una nueva.
3. En el panel derecho, en **Acciones**, en el campo **Ejecutar tarea o trabajo**, haga clic en **Seleccione un trabajo o tarea**.
4. En el cuadro de diálogo **Seleccionar una tarea**, en el panel izquierdo, seleccione el trabajo o la tarea apropiado y después haga clic en **Aceptar**.

   Ver "Seleccionar trabajo o tarea para la política de automatización" en la página 404.
5. (Opcional) Haga clic en **Editar parámetro de entrada** y, a continuación, en el cuadro de diálogo Editar parámetros de entrada del trabajo o tarea, especifique lo siguiente para cada parámetro de la acción:

Origen de datos	El campo de origen de datos que suministra el parámetro. Seleccione la opción apropiada de la lista desplegable: ■ Resultados como HTML ■ Resultados como CSV ■ Resultados como texto ■ Número de filas ■ Personalizado(a)
Valor personalizado	El valor que se usa cuando el origen de datos se configura como Personalizado. Este valor es la opción predeterminada que se usa si el campo especificado de origen de datos no está disponible.

Este campo no se muestra si no se requiere ningún parámetro de la entrada.

6 (Opcional) Haga clic en **Aceptar** para cerrar la ventana Editar parámetros de entrada del trabajo o tarea.

7 Haga clic en **Guardar cambios**.

Seleccionar trabajo o tarea para la política de automatización

El cuadro de diálogo **Seleccionar una tarea** permite seleccionar el trabajo o la tarea que se realizará cuando se active la política de automatización.

Ver "Especificación de una acción de política de automatización" en la página 402.

El panel izquierdo visualiza la estructura de la carpeta Administración de tareas y contiene todas las tareas disponibles para su uso en las políticas de automatización. El panel derecho muestra la página de configuración de tareas para la tarea seleccionada y permite realizar cualquier cambio necesario.

Para seleccionar un trabajo o una tarea para la política de automatización

1 En Symantec Management Console, en el menú **Administrar**, haga clic en **Políticas de automatización**.

2 En la página **Políticas de automatización**, en la ficha **Mensajes del sistema**, seleccione una política de automatización existente o cree una nueva.

3 En el panel derecho, en **Acciones**, en el campo **Ejecutar tarea o trabajo**, haga clic en **Seleccione un trabajo o tarea**.

4 En el cuadro de diálogo **Seleccionar una tarea**, en el panel izquierdo, seleccione el trabajo o la tarea apropiada y luego en el panel derecho, realice cualquier cambio de configuración necesario al trabajo o a la tarea.

5 Haga clic en **Aceptar**.

Creación y modificación de tareas de políticas de automatización

Con Symantec Management Platform, se proporciona un conjunto de tareas de políticas de automatización. Puede utilizarlas en sus políticas de automatización y también como plantilla para crear sus propios trabajos y tareas personalizados.

Ver "Especificación de una acción de política de automatización" en la página 402.

Las políticas le permiten realizar las acciones siguientes:

Asignar a grupo organizativo	Le permite asignar recursos a un grupo organizativo.
Enviar por correo electrónico un informe	Le permite enviar por correo electrónico un informe especificado como archivo adjunto. Puede utilizar esta tarea como parte del trabajo que también incluye Ejecutar una tarea de informe para crear el informe apropiado.
Enviar un correo electrónico	Le permite enviar un correo electrónico con la información que se define a los usuarios especificados. El correo electrónico puede incluir el estado, la licencia del producto u otra información.
Ejecutar un informe	Es posible que desee utilizar esta tarea como parte de un trabajo que además incluye una tarea de informe por correo electrónico para enviar el informe al administrador de Notification Server o los usuarios apropiados

Para crear o modificar una tarea de política de automatización

1. En Symantec Management Console, en el menú **Administrar**, haga clic en **Tareas y trabajos**.
2. En el panel izquierdo, expanda la carpeta **Tareas y trabajos > Trabajos y tareas de sistema > Notification Server > Tareas de políticas de automatización** y después realice una de las siguientes acciones:

Para crear un trabajo o una tarea nuevos desde el comienzo	1 Haga clic con el botón derecho en la carpeta **Tareas de políticas de automatización**, haga clic en **Nueva** y después haga clic en la opción apropiada. 2 En el cuadro de diálogo **Crear una nueva tarea**, en el panel izquierdo, seleccione la tarea. 3 En el panel derecho, especifique las opciones y después haga clic en **Aceptar**.

Para crear un trabajo o una tarea nuevos usando un trabajo o una tarea existentes como plantilla	Haga clic con el botón derecho en el trabajo o la tarea y después haga clic en **Clonar**.
Para modificar un trabajo o una tarea existentes	Haga clic en el trabajo o la tarea.

3 En el panel derecho, especifique los detalles apropiados para el trabajo o la tarea.

4 Haga clic en **Guardar cambios**.

Capítulo 26

Usar las tareas y los trabajos

En este capítulo se incluyen los temas siguientes:

- Acerca de la administración de tareas
- Componentes de administración de tareas
- Cómo Task Server usa el mecanismo de señal
- Cuándo usar tareas, trabajos y políticas
- Acerca de cómo ejecutar tareas en jerarquía
- Secuenciación de tareas
- Cómo consultar y editar permisos en un tipo de tarea
- Creación de tareas para introducir o mostrar las propiedades de la tarea
- Cómo limpiar datos de tarea
- Limpiar datos de la versión de la tarea
- Cómo cambiar la configuración de Client Task Agent
- Acceder al Portal de trabajos y tareas

Acerca de la administración de tareas

La Administración de tareas proporciona la secuenciación y la automatización de tareas para las soluciones de Symantec. La secuenciación de tareas permite realizar operaciones de administración complejas en un único trabajo. Las tareas se pueden ordenar en un trabajo, lo que proporciona gran flexibilidad en el trabajo. La

funcionalidad es similar a la que provee el software Symantec Deployment Solution con el motor de trabajo. Sin embargo, Symantec Management Platform aprovecha la Administración de tareas y permite al resto del catálogo de soluciones de Symantec emplear sus funciones eficaces.

Ver "Secuenciación de tareas" en la página 416.

Es posible ejecutar automáticamente las tareas basadas en eventos en el sistema o cambios en la base de datos. Es posible también ejecutar tareas automáticamente para que los equipos sigan cumpliendo con las políticas.

Los equipos con Task Server son similares a los servidores de paquetes en que están diseñados para residir en un servidor separado y son muy ligeros. Tanto los equipos con Task Server como los servidores de paquetes son servicios de sitio y se instalan en un servidor de sitio. Los equipos se pueden asignar a un servidor de sitio específico por nombre de equipo o por subred.

Ver "Acerca de los servicios de sitio" en la página 127.

Es posible crear, ejecutar o programar trabajos y tareas del portal de trabajos y tareas. Los componentes de tarea coordinan estos trabajos y tareas eficazmente.

Ver "Componentes de administración de tareas" en la página 409.

La administración de tareas incluye las siguientes funciones:

- Ejecuta varias tareas en una secuencia definida que se denomina trabajo.
  Ver "Cómo crear un trabajo" en la página 418.
- Permite a los usuarios proporcionar lógica para controlar los errores u otros códigos de retorno.
- Incluye una línea de comandos eficaz y capacidades de VBscript.
- Proporciona las tareas de administración de energía predefinidas.
- Ejecuta las tareas de cliente y servidor.
  Ver "Implementación de un Task Server" en la página 417.
- Proporciona las funciones de acción rápida para los trabajos en ejecución, como las opciones Ejecutar ahora y comentarios del estado prácticamente en tiempo real.
  Ver "Ejecución de un trabajo o una tarea" en la página 421.
  Ver "Adición de una programación a una política, una tarea o un trabajo" en la página 424.
  Ver "Cómo ver el estado de tarea en Symantec Management Agent" en la página 425.
- Reutiliza las tareas en varios trabajos o permite clonar y modificar tareas según lo desee.

Componentes de administración de tareas

Trabajos de Administración por medio de varios componentes. Estos componentes coordinan la asignación y el rendimiento de tareas y de trabajos en los equipos cliente conectados.

Ver "Acerca de la administración de tareas " en la página 407.

Tabla 26-1 Componentes de administración de tareas

Componente	Descripción
Task Server	Este componente distribuye trabajos y tareas en la red y se puede ejecutar en Notification Server o en un equipo remoto. Task Server tiene la capacidad de mandar una señal a los equipos cliente registrados. Esta capacidad de señalización se encuentra separada del componente del servidor de señales en el equipo con Notification Server. Task Server envía la información de estado al cargador de datos. Además envía las señales, el trabajo y la información de la tarea a Client Task Agent.
Servidor de señales	El servidor de señales notifica a Task Server cuando hay tareas para ejecutar en los equipos cliente conectados. Luego, manda una señal a los equipos cliente conectados y les envía el XML que contiene la información sobre el trabajo o la tarea a través de HTTP(S). El servidor de señales también recopila información sobre el estado y la envía a la Base de datos de la administración de configuración (CMDB) través de HTTP(S). Este componente siempre se ejecuta en el equipo con Notification Server. Envía un paquete de señales de IP a los Task Servers cada vez que sus clientes tienen un trabajo o una tarea para ejecutar. Ver "Cómo Task Server usa el mecanismo de señal" en la página 410.
Cargador de datos	Este componente recibe información sobre el estado de los servidores de tareas y la almacena en la memoria caché hasta que pueda enviarlos a CMDB. El cargador de datos mejora la escalabilidad, ya que permite recibir información sobre el estado de varios cientos de clientes a la vez sin sobrecargar el SQL Server. Además, este componente se ejecuta en cada Task Server remoto y pone en cola los datos que están en espera hasta que puedan ser enviados a Notification Server.

Componente	Descripción
Agente de tareas del cliente	Este agente se ejecuta en equipos cliente y realiza las siguientes acciones: ■ Acepta señales de Task Server. ■ Recibe la información del trabajo y de la tarea. ■ Pasa la información a un controlador. ■ Envía nuevamente la información sobre el estado de Task Server. Este agente se instala automáticamente con Symantec Management Agent. **Nota:** Cuando instala Symantec Management Agent en un equipo, existe un retraso antes de que Client Task Agent se registre con Notification Server. Cualquier tarea que se realice en el equipo durante este tiempo (aproximadamente 10 minutos) tiene el estado pendiente hasta que Client Task Agent se registre. Cuando se registra Client Task Agent, las tareas se ejecutan de forma inmediata.

Cómo Task Server usa el mecanismo de señal

El servidor de señales es un componente de Administración de tareas. El componente del servidor de señales se ejecuta solamente en el equipo con Notification Server y es responsable de notificar a Task Server las tareas pendientes para los equipos clientes. Task Server también cuenta con una capacidad plena para señalizar los equipos clientes registrados. Esta capacidad de señalización se encuentra separada del componente del servidor de señales en el equipo con Notification Server.

Ver "Componentes de administración de tareas" en la página 409.

El servidor de señales envía un paquete de señales de IP a los Task Servers cada vez que sus equipos clientes registrados tienen un trabajo o una tarea para ejecutar. Tras la recepción del paquete de señales, Task Server solicita de manera inmediata a Notification Server la información de la tarea o el trabajo para sus equipos clientes registrados. También señaliza los equipos clientes. Cuando el Agente de tareas del cliente recibe el paquete de señales, solicita la información del trabajo o la tarea de Task Server registrado. La tarea se ejecuta solamente después de que el Agente de tareas del cliente recibe la información de la tarea. Los eventos de estados de las tareas completadas se envían nuevamente al Task Server registrado después de haberse completado.

Si los paquetes de señales están bloqueados o, por alguna otra razón, no pueden llegar a destino, el Agente de tareas del cliente comprueba de forma automática el Task Server registrado para cualquier información de trabajo nuevo. Lleva a cabo esta comprobación cada 5 minutos. Este intervalo de solicitud de la tarea es configurable en Symantec Management Console. La información de tarea o trabajo de Task Server no se recibe mediante la política de configuración de Symantec Management Agent. Se recibe directamente por el Agente de tareas del cliente de Task Server registrado. Si fuerza a Symantec Management Agent a actualizar su política de configuración, esto no obliga al Agente de tareas del cliente a recibir información de tareas pendientes.

Ver "Cómo cambiar la configuración de Client Task Agent" en la página 430.

De manera predeterminada, el servidor de señales utiliza el puerto 50123 para servidores de tarea, y los Task Servers utilizan el puerto 50124 para señalizar Agentes de tareas del cliente.

Ver "Acerca de la administración de tareas " en la página 407.

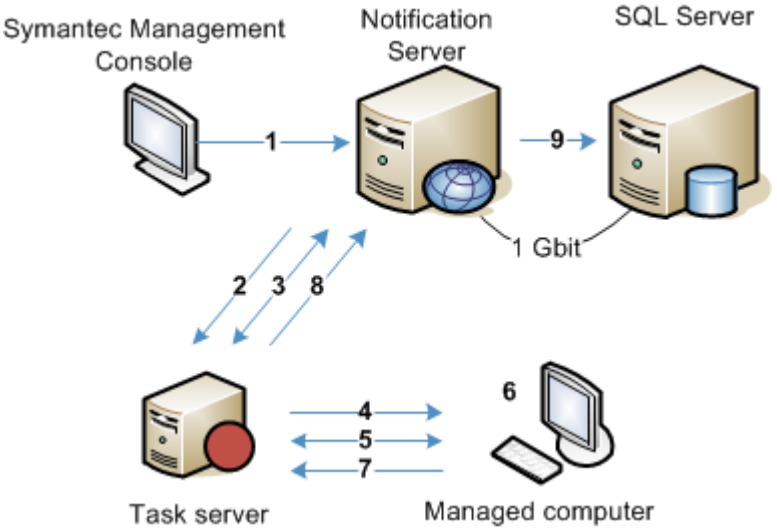
El siguiente ejemplo supone que el Client Task Agent para el equipo A está registrado con Task Server remoto1.

Tabla 26-2 Secuencia de funcionamiento de la señal de Task Server

Secuencia	Descripción
Uno	Un administrador de Notification Server asigna una tarea para que esta se ejecute de forma inmediata en el equipo A.
Dos	El servidor de señales en el equipo con Notification Server envía un paquete de señales para avisar a RemoteTaskServer1 sobre la tarea pendiente.
Tres	RemoteTaskServer1 verifica si el cliente de destino tiene permitido recibir cualquier tarea. Si se deshabilita el modo **Comunicación de agente de una versión anterior** y el destino es un agente de una versión anterior, la tarea falla de forma inmediata. Además falla si se actualiza el agente, pero está en estado **No permitido**. Ver "Acerca del registro de agente" en la página 237.
Cuatro	RemoteTaskServer1 recibe el paquete de señales y solicita de forma inmediata la información del trabajo de Notification Server.
Cinco	RemoteTaskServer1 señaliza el equipo A para notificarlo de la tarea pendiente.

Secuencia	Descripción
Seis	El equipo A recibe el paquete de señales y solicita de manera inmediata la información del trabajo del Task Server registrado - RemoteTaskServer1.
Siete	El equipo A recibe la información de trabajo y ejecuta la tarea.
Ocho	Una vez que la tarea se ha completado, el equipo A vuelve a enviar un evento de estado a RemoteTaskServer1.
Nueve	RemoteTaskServer1 almacena el evento de estado e inmediatamente intenta volver a enviarlo a Notification Server.
Diez	Notification Server recibe el evento de estado de RemoteTaskServer1 y registra la información en la base de datos.

Figura 26-1 Secuencia de funcionamiento de la señal de Task Server



Cuándo usar tareas, trabajos y políticas

Las tareas, los trabajos y las políticas tienen diferente usos en Notification Server. Cuál se usa depende de lo que se desee conseguir.

Una política es un conjunto de reglas que se aplica a un recurso o a un grupo de recursos (conocido como el destino de la política). Una política se puede evaluar sobre la base de una programación o de datos entrantes. Cuando se evalúa una

política, se aplica la acción apropiada. Esta acción incluye típicamente la ejecución de tareas en los recursos de destino para garantizar que todos cumplan con la política. Usar una política le permite aplicar acciones a los recursos determinados, que se definen como destino de la política.

Ver "Acerca de las políticas de Symantec Management Platform" en la página 376.

Una tarea es una acción aparte que no tiene acciones continuadas y que se implementa a los equipos seleccionados. Es posible ejecutar automáticamente las tareas basadas en eventos en el sistema o cambios en la base de datos. Es posible también ejecutar tareas automáticamente para que los equipos sigan cumpliendo con las políticas.

Un trabajo es una secuencia de tareas que se ejecutan en un orden específico.

Ver "Acerca de la administración de tareas " en la página 407.

En general, las políticas se usan para administración continua; las tareas, para aplicar políticas o realizar acciones una vez.

Tabla 26-3 Cuándo usar tareas, trabajos y políticas

Opción	Criterio
Tarea	Use una tarea cuando los criterios siguientes sean verdaderos: ■ Es necesario realizar una acción que finalice rápidamente (sin acciones continuas).
Trabajo	Use un trabajo cuando los criterios siguientes sean verdaderos: ■ Es necesario ejecutar acciones en un orden específico. ■ Una acción puede ser útil para que un usuario final ordene en secuencia o relacione un mensaje de Notification Server.
Política	Use una política cuando los criterios siguientes sean verdaderos: ■ Tiene datos de configuración estáticos para enviar a Symantec Management Agent. ■ Tiene acciones continuadas sin fin definido.

Acerca de cómo ejecutar tareas en jerarquía

Symantec Management Platform le permite crear tareas en el Notification Server principal y ejecutarlas en todos los equipos cliente en la jerarquía. Tales tareas además se replican en el Notification Server secundario y se ejecutan en todos los equipos administrados aplicables.

Ver "Acerca de la jerarquía de Notification Server" en la página 153.

Ver "Acerca de la administración de tareas " en la página 407.

Cuando se ejecutan tareas en jerarquía, es necesario considerar los siguientes aspectos específicos del diseño:

Los equipos cliente informan sobre el estado de las tareas solamente al Notification Server al cual están asignados. La información de estado de las tareas para los equipos cliente que están asignados a un Notification Server secundario no es siempre exacta en el Notification Server principal.	Si crea una tarea en el Notification Server principal y la ejecuta en todos los equipos cliente de su entorno, no todos los equipos informan al Notification Server principal. Los equipos cliente que están asignados al Notification Server secundario informan sobre el estado de las tareas solamente al Notification Server secundario. Además, la información de estado de las tareas no se replica del Notification Server secundario al principal. Por lo tanto, la página **Trabajos o tareas** de Notification Server principal muestra información inexacta del estado de las tareas que se ejecutan en los equipos cliente asignados a un Notification Server secundario. Es posible ver la información inexacta del estado de las tareas de cada equipo por separado en el Notification Server principal, en la ventana **Detalles de instancia de tarea**. Tenga en cuenta que la ventana **Detalles de instancia de tarea** abre una URL del Notification Server secundario y requiere las credenciales del Notification Server secundario. Además, la ventana **Detalles de instancia de tarea** muestra la información correcta del estado de las tareas solamente en los casos siguientes: ■ Si crea una tarea en el Notification Server principal, haga clic en **Ejecución rápida** o **Nueva programación > Ahora** y agregue los equipos cliente del Notification Server secundario como destino de esta tarea. ■ Si crea una tarea en el Notification Server principal, agregue una programación para la tarea y agregue los equipos cliente del Notification Server secundario como destino de esta tarea. Tenga en cuenta que si se replica la tarea al Notification Server secundario e inicia la tarea desde allí, no podrá ver los detalles de estado de la tarea en el Notification Server principal.

El trabajo del servidor que contiene las tareas de cliente no se replica correctamente del Notification Server principal a su servidor secundario.	Si crea un trabajo de servidor que contenga tareas de cliente y las replica de un Notification Server principal a su servidor secundario, las tareas de cliente dentro del trabajo del servidor se replicarán al Notification Server secundario, pero las tareas del servidor y el trabajo del servidor en sí mismo no se replicarán. Además, las tareas del servidor de ese trabajo determinado se ejecutan en el Notification Server principal, mientras que las tareas de cliente se ejecutan en el Notification Server secundario. Para solucionar este problema, puede crear un trabajo de servidor en el Notification Server secundario y agregarle las tareas de cliente replicadas. Alternativamente, puede crear un trabajo de cliente en el servidor principal. El trabajo de cliente que contiene las tareas de cliente se replica correctamente. Si aplica un trabajo de servidor que contiene tareas de cliente del Notification Server principal al Notification Server secundario, el estado de ejecución del trabajo estará disponible solamente en el Notification Server principal. En el Notification Server secundario, la instancia de ese trabajo determinado no se crea. Tenga en cuenta que Symantec no recomienda el crear de un trabajo de servidor que contenga tareas de cliente. Para obtener más información sobre los trabajos y las tareas, consulte el siguiente artículo de la base de conocimientos: http://www.symantec.com/docs/HOWTO9671
Si elimina la tarea del Notification Server principal, la opción **Replicar ahora** no elimina esta tarea en el Notification Server secundario.	Si elimina una tarea del Notification Server principal y usa la opción **Replicar ahora** para replicar esta operación al Notification Server secundario, la tarea no se elimina del Notification Server secundario. Solamente la replicación diferencial o completa elimina la tarea correctamente del Notification Server secundario.
Para los trabajos que contienen solamente tareas servidor y para las tareas de servidor, la programación no se replica del Notification Server principal al secundario.	Si crea y programa una nueva tarea de servidor en el Notification Server principal y después la replica en el Notification Server secundario, la programación no se replica en el secundario. Es necesario programar esta tarea por separado en el Notification Server secundario.

Secuenciación de tareas

La secuenciación de tareas permite realizar operaciones de administración complejas en un único trabajo. Las tareas se pueden ordenar en un trabajo, lo que proporciona gran flexibilidad en el trabajo.

Ver "Acerca de la administración de tareas " en la página 407.

Tabla 26-4 Proceso para la secuenciación de tareas

Paso	Acción	Descripción
Paso 1	(Opcional) Implemente equipos Task Server.	Los equipos Task Server permiten distribuir trabajos y tareas a los equipos de su red. De esta manera, los trabajos y las tareas pueden ejecutarse en equipos administrados. Symantec recomienda implementar por lo menos un Task Server por Notification Server. Una vez implementado el Task Server dedicado inicial, agregue Task Servers adicionales para cada 5000 a 7500 equipos cliente. La cantidad de equipos administrados que un Task Server puede servir depende del hardware del equipo Task Server. Ver "Implementación de un Task Server" en la página 417.
Paso 2	Cree una tarea.	Tareas que se ejecuten en Notification Server o en equipos administrados. Ver "Cómo crear una tarea" en la página 418.
Paso 3	Cree un trabajo.	Los trabajos ejecutan tareas, otros trabajos y condiciones. Ver "Cómo crear un trabajo" en la página 418.
Paso 4	Ejecute trabajos o tareas.	Los trabajos y las tareas se pueden ejecutar en Notification Server o en equipos administrados. Ver "Ejecutar un trabajo o una tarea usando arrastrar y soltar" en la página 420. Ver "Ejecución de un trabajo o una tarea" en la página 421. Ver "Volver a ejecutar una tarea con errores" en la página 422. Ver "Adición de una programación a una política, una tarea o un trabajo" en la página 424.

Paso	Acción	Descripción
Paso 5	Consulte el estado en tiempo real de los trabajos o de las tareas.	Es posible ver el estado del trabajo o de la tarea en Symantec Management Console y además en un equipo cliente, en Symantec Management Agent. **Nota:** Para mejorar el rendimiento, en Symantec Management Console, el estado de la tarea se actualiza cada cinco minutos. Ver "Cómo ver el estado de tarea en Symantec Management Agent" en la página 425.

Implementación de un Task Server

Los Task Servers le permiten distribuir los trabajos y las tareas en distintos equipos de la red donde los Symantec Management Agents pueden ejecutar trabajos y tareas. Cuando se distribuyen los trabajos y las tareas, se reduce el tráfico de red y la carga en Notification Server. Symantec Management Agent accede al Task Server más cercano para la descarga de trabajos y tareas.

Ver "Componentes de administración de tareas" en la página 409.

Cada Notification Server se convierte en un Task Server cuando el componente de Task Server está instalado. Es posible entonces implementar más Task Servers, según las necesidades.

Task Server se puede instalar solamente en un equipo que tenga IIS instalado.

Los requisitos para un equipo Task Server son las siguientes:

- Microsoft .NET Framework, versión 3.5
- Los sistemas operativos que mínimamente se admiten son Windows XP x86 SP3, Windows x64 SP2 o Windows Server 2003 SP2
- Microsoft Internet Information Services (IIS)
- Symantec Management Agent

Las recomendaciones mínimas del hardware para un equipo Task Server son las siguientes:

- Procesador Intel Pentium 4 o equivalente
- 1-GB de RAM
- Espacio libre en disco de 1 GB

Symantec recomienda implementar por lo menos un Task Server por Notification Server. Una vez implementado el Task Server dedicado inicial, agregue Task

Servers adicionales para cada 5000 a 7500 equipos cliente. La cantidad de equipos administrados que un Task Server puede servir depende del hardware del equipo Task Server.

Ver "Acerca de los servicios de sitio" en la página 127.

Esta tarea es un paso en el proceso para ordenar las tareas.

Ver "Secuenciación de tareas" en la página 416.

Para implementar Task Server utilizando servicios de sitio

- Implementar Task Server como servidor de sitio.

  Ver "Administración de servidores de sitio" en la página 131.

Cómo crear una tarea

Se crean e implementan tareas en equipos administrados usando tipos predefinidos de tareas. El tipo de tarea que se elige depende de qué se desea hacer. Muchos tipos de tareas se proporcionan con la Administración de tareas. Algunas soluciones de Symantec además proporcionan tipos de tarea y trabajos de muestra.

Esta tarea es un paso en el proceso para ordenar las tareas.

Ver "Secuenciación de tareas" en la página 416.

Para crear una tarea

1. En Symantec Management Console, en el menú **Administrar**, haga clic en **Tareas y trabajos**.
2. En el panel izquierdo, haga clic con el botón derecho en la carpeta donde desee crear la tarea y haga clic en **Nueva > Tarea**.
3. En el cuadro de diálogo **Crear una nueva tarea**, en el panel izquierdo, seleccione el tipo de tarea.
4. En el panel derecho, configure la tarea.
5. Haga clic en **Aceptar**.

Cómo crear un trabajo

Es posible crear trabajos que ejecuten varias tareas o trabajos. Los dos tipos de trabajos son trabajos de servidor y trabajos de cliente. Los trabajos de servidor se ejecutan en Notification Server. Los trabajos de cliente se implementan en equipos administrados mediante Task Server. El equipo administrado ejecuta el trabajo y envía informes a Notification Server.

Los trabajos pueden contener varios trabajos, tareas y condiciones, lo que brinda gran flexibilidad al configurar la secuencia de trabajos que necesita.

Esta tarea es un paso en el proceso para ordenar las tareas.

Ver "Secuenciación de tareas" en la página 416.

Para crear un trabajo

1. En Symantec Management Console, en el menú **Administrar**, haga clic en **Tareas y trabajos**.
2. En el panel izquierdo, haga clic con el botón derecho en la carpeta donde desee crear la tarea y después haga clic en **Nuevo > Trabajo de servidor** o **Nuevo > Trabajo del cliente**.
3. En el panel derecho, configure el trabajo:

Edite el nombre del trabajo	Haga clic en el texto del nombre y escriba el nuevo nombre.
Cree una nueva tarea para agregar a un trabajo	1 Haga clic en **Nueva > Tarea**. 2 En el cuadro de diálogo **Crear tarea nueva**, en el panel izquierdo, seleccione una tarea. 3 En el panel derecho, configure la tarea. 4 Haga clic en **Aceptar**.
Agregue una tarea o un trabajo existente a un trabajo	1 Haga clic en **Agregar existente**. 2 En el cuadro de diálogo **Agregar tarea existente**, en el panel izquierdo, seleccione la tarea o el trabajo que desee agregar. 3 Haga clic en **Aceptar**. Está disponible la función de arrastrar y soltar, que permite cambiar el orden de las tareas o los trabajos que se agregan al trabajo. También es posible usar las flechas hacia arriba y abajo del menú para mover tareas, trabajos y condiciones.

Agregue una condición a un trabajo

1. Haga clic en **Nueva > Condición**.
2. En el cuadro de diálogo **Editar condición**, la regla da una cláusula **dónde** que le permite seleccionar una tarea o un trabajo, una operación para realizar y una condición para realizar la operación en la tarea o el trabajo.
3. En la primera lista desplegable, seleccione o escriba la tarea o el trabajo y el código de retorno de la condición.
4. En la segunda lista desplegable, seleccione la operación para que la regla realice.
5. En el tercer campo, escriba la condición.
6. (Opcional) Para agregar más reglas, haga clic en **Agregar regla**.
7. Haga clic en **Aceptar**.

Es posible agregar una o más tareas o trabajos para ejecutar como resultado de la condición en **Si no**.

4 Haga clic en **Guardar cambios**.

Ejecutar un trabajo o una tarea usando arrastrar y soltar

En la vista mejorada **Trabajos o tareas**, puede ver, ejecutar y programar fácilmente tareas y trabajos.

Ver "Acerca de la vista Trabajos o tareas " en la página 44.

Es posible también ejecutar trabajos y tareas arrastrándolos y soltándolos en uno o más equipos. Puede también usar la opción **Ejecución rápida** para señalar un trabajo o una tarea sin explorar los niveles inferiores manualmente.

Ver "Especificación de destinos de una política o tarea" en la página 379.

Nota: Es necesario tener uno de los siguientes conjuntos de aplicaciones o soluciones instalados para realizar esta tarea: Deployment Solution (producto independiente), IT Management Suite, Server Management Suite o Client Management Suite.

Para ejecutar un trabajo o una tarea usando arrastrar y soltar

1. En Symantec Management Console, en el menú **Administrar**, haga clic en **Tareas y trabajos**.
2. En el panel de navegación, haga clic en la tarea o el trabajo que desea ejecutar y arrástrelo a la derecha para iniciar la operación de arrastrar y soltar.

   Los resultados de la búsqueda informática más reciente aparecen en el panel de lista. Si filtró la búsqueda informática más actual, la lista muestra los resultados de la búsqueda filtrada.

   Ver "Buscar un equipo y guardar la búsqueda como filtro" en la página 39.
3. Para seleccionar los equipos en los cuales desea ejecutar el trabajo o la tarea, realice una de las siguientes acciones:
   - Para ejecutar el trabajo o la tarea en todos los equipos enumerados, suéltelo en el pequeño icono de título en el panel de lista.
   - Para ejecutar el trabajo o la tarea en un equipo específico, suéltelo en el equipo de la lista.
   - Para ejecutar un trabajo o tarea en una búsqueda guardada, vista organizativa o grupo organizativo, arrástrelo a la hoja **Equipos** y, a continuación, suéltelo en una búsqueda guardada, una vista organizativa o un grupo organizativo.
4. En el cuadro de diálogo **Nueva programación**, especifique la programación del trabajo o de la tarea y después haga clic en **Programación**.

Ejecución de un trabajo o una tarea

Los trabajos y las tareas que crea se pueden ejecutar en Notification Server o en los equipos administrados dependiendo de si son tareas de servidores o tareas del cliente. Las tareas de servidor son las tareas que se ejecutan en un equipo Notification Server. Las tareas de cliente son las tareas que se ejecutan en un equipo cliente.

Si más de una tarea se agrega a un trabajo, se agrega una tras otra. Si se agrega una condición, las tareas que se realizan se basan en los resultados de la condición. El servidor debe recibir el estado de una tarea anterior que se ha completado antes de que se inicie la siguiente tarea en el trabajo. Es posible que se produzca un retraso de algunos segundos antes de que la siguiente tarea comience.

Esta tarea es un paso en el proceso para ordenar las tareas.

Ver "Secuenciación de tareas" en la página 416.

Para ejecutar un trabajo o una tarea

1. En Symantec Management Console, en el menú **Administrar**, haga clic en **Tareas y trabajos**.
2. En el panel izquierdo, seleccione el trabajo o la tarea que desee ejecutar.
3. Agregue una programación para ejecutar el trabajo o la tarea.

   Ver "Adición de una programación a una política, una tarea o un trabajo" en la página 424.

Volver a ejecutar una tarea con errores

Es posible volver a ejecutar una tarea en los equipos con errores.

Ver "Acerca de la administración de tareas " en la página 407.

La reejecución de la tarea funciona de la siguiente manera:

- Es posible seleccionar varias instancias de la tarea para volver a ejecutar. Todos los equipos con errores de las instancias incluidas de la tarea se incluyen en la instancia de la tarea de reejecución.
- Es posible volver a ejecutar solamente tareas con errores de equipos cliente, no tareas con errores de servidor.
- **Volver a ejecutar instancias con errores** omite cualquier destino que fue usado en la instancia anterior de la tarea sin importar cómo fue creada (ejecución rápida, programación en una lista de equipos o programación en un destino). Vuelve a ejecutar en la lista de equipos con errores a partir de la tarea que acaba de ejecutar.

Nota: Use la función de volver a ejecutar la tarea solamente en el nivel del Notification Server secundario, donde se pueden ver los indicadores de estado de la tarea. Recomendamos que usted no vuelva a ejecutar las tareas desde un Notification Server principal en una jerarquía debido a los retrasos en replicar los datos.

Para volver a ejecutar una tarea con errores

1 En Symantec Management Console, en el menú **Administrar**, haga clic en **Equipos**.

Nota: Es posible también ir directamente a **Administrar > Tareas y trabajos** y omitir los pasos 2 y 3.

---

2 Haga clic en las flechas dobles (>>) en la parte superior del panel de lista para ir al resumen del contenedor de **Entregas de software**.

3 En **Tareas de Entrega rápida**, haga clic en una instancia de una tarea que haya tenido errores en algunos de los equipos y que se desea volver a ejecutar en esos equipos.

4 En el panel **Estado de tarea**, haga clic en **Volver a ejecutar instancias con errores** para volver a ejecutar las instancias de la tarea en la lista de equipos que devolvieron un estado **Con error**.

5 Esta acción inicia la ventana **Nueva programación**. Completa previamente el campo **Dispositivos seleccionados** con los equipos donde las instancias de la tarea no pudieron ejecutarse.

Nota: Si hace clic en **Volver a ejecutar instancias con errores** en una instancia de la tarea sin equipos con error, un mensaje emergente indica que no hay equipos con error con esta instancia de la tarea. Cuando haga clic en **Volver a ejecutar instancias con errores** en una instancia de la tarea que esté en un estado pendiente o en ejecución, no se detallan equipos, porque la tarea no se ha realizado correctamente ni ha fallado aún.

---

6 Haga clic **Programación** para programar la tarea para volver a ejecutarla en los equipos con error.

Esto crea una nueva instancia de la tarea. La instancia anterior aún está allí.

Nota: Es posible que encuentre un mensaje de error que lea: “Esta ejecución de tarea se ha eliminado y no se puede ver ni volver a ejecutar. Solo hay datos de resumen.” Administración de tareas tiene una tarea diaria de limpieza que se ejecuta según las especificaciones de usuario para limitar la cantidad de filas en funcionamiento en la base de datos. Esto evita que el rendimiento de Administración de tareas se ralentice demasiado. De forma predeterminada, cada noche, la tarea de la limpieza conserva solamente las 200,000 instancias más recientes de la tarea. El recuento de equipos sigue mostrando todos los equipos en que fue ejecutada la tarea. Sin embargo, si los detalles de alguna de esas instancias de la tarea se han eliminado, **Volver a ejecutar instancias con errores** no incluye esas tareas. Como consecuencia, puede haber una discrepancia entre el recuento de equipos donde la tarea falló y el recuento cuando haga clic en **Volver a ejecutar instancias con errores**.

---

7 Esta nueva programación ahora aparecerá en la página del folioscopio de **Entregas de software**. Es posible ver qué instancia de la tarea se ejecutó o se volvió a ejecutar más recientemente. Es posible también ver en cuántos equipos se ejecutó la tarea correcta o incorrectamente.

Adición de una programación a una política, una tarea o un trabajo

Cuando programa una política, una tarea o un trabajo para que se ejecute, tiene dos opciones: ejecución rápida y programación. La opción Ejecución rápida ejecuta la política o el trabajo actual de forma inmediata en un equipo que se especifica. La opción Programación proporciona varias opciones de equipos de programación y de destino. La opción Programación le permite establecer una programación. El destino se debe definir en otro lugar.

Para agregar una programación de ejecución rápida

1 En Symantec Management Console, en el menú **Administrar**, haga clic en **Tareas y trabajos**.

2 En el panel izquierdo, seleccione la política, el trabajo o la tarea al que desea aplicar la ejecución rápida.

3 En el panel derecho, en **Estado de tarea**, haga clic en **Ejecución rápida**.

4 En el cuadro de diálogo **Ejecución rápida ahora**, seleccione el nombre del equipo en el cual desea ejecutar la política, la tarea o el trabajo.

5 Haga clic en **Ejecutar**.

Para agregar una programación nueva

1 En Symantec Management Console, en el menú **Administrar**, haga clic en **Tareas y trabajos**.

2 En el panel izquierdo, seleccione la política, el trabajo o la tarea que desea programar.

3 En el panel derecho, en **Estado de tarea**, haga clic en **Nueva programación**.

4 En el cuadro de diálogo **Nueva programación**, configure la programación.

5 Haga clic en **Programar**.

Cuando se seleccionan tareas o trabajos para ser ejecutados, aparecen en la sección Estado de trabajos y tareas.

Cómo ver el estado de tarea en Symantec Management Agent

El estado de tareas (incluido el historial de tareas) se registra en Symantec Management Agent. Para ver el estado de tarea en un equipo, abra Symantec Management Agent. El estado de tarea permite ver qué tareas se han ejecutado y los resultados de las mismas.

Esta tarea es un paso en el proceso para ordenar las tareas.

Ver "Secuenciación de tareas" en la página 416.

Para ver el estado de tarea en Symantec Management Agent

1 En el equipo que desee para ver el estado, haga doble clic en el icono en la bandeja del sistema para abrir Symantec Management Agent.

2 En la ventana **Symantec Management Agent**, haga clic en la ficha **Estado de tarea**.

Cómo consultar y editar permisos en un tipo de tarea

Es posible consultar y editar los permisos en propiedades del tipo de tarea. Cambiar permisos en el tipo de tarea le permite controlar qué usuarios pueden crear tareas. Los usuarios que tienen el permiso de para Crear una nueva tarea pueden crear tareas de ese tipo.

Ver "Acerca de la administración de tareas " en la página 407.

Ver "Secuenciación de tareas" en la página 416.

Ver "Categorías de permisos de seguridad" en la página 491.

Ver "Permisos de Task Server" en la página 506.

Para ver y editar permisos en un tipo de tarea

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Todas las configuraciones**.
2. En el panel izquierdo, haga clic en **Notification Server > Configuración de tarea > Tipos de tareas**.
3. Vaya al tipo de tarea que usted quiere ver y después haga clic sobre ella.
4. En el panel derecho, haga clic en **Ver permisos**.
5. Para editar permisos, en Administrador de roles de seguridad, edite los permisos en el tipo de tarea.

   Ver "Asignación de permisos de seguridad a carpetas y elementos" en la página 103.

Creación de tareas para introducir o mostrar las propiedades de la tarea

Las propiedades de entrada son las propiedades que pasan a una tarea de cierto origen. Las tareas pueden recibir propiedades de entrada desde un valor determinado, desde otras tareas o en el momento de ejecución. Las tareas pueden usar estas propiedades de la entrada (similares a las variables) para realizar sus funciones. Todas las propiedades que están disponibles para una tarea (las propiedades de la entrada y las propiedades que crea la tarea) se denominan propiedades de la tarea.

Una tarea puede enviar sus propiedades de la tarea a otras tareas. Si tiene una tarea que envíe propiedades, cualquier tarea subsiguiente de ese trabajo puede usar esas propiedades de la salida para sus propiedades de la entrada. Las tareas no necesitan ser simultáneas.

No necesita una tarea de salida para cada tarea de entrada. Las tareas de entrada pueden, además, recibir información desde un valor determinado o en el momento de ejecución.

Ver "Acerca de la administración de tareas " en la página 407.

Ver "Cómo crear una tarea" en la página 418.

Para crear una tarea que envíe propiedades

1. En Symantec Management Console, en el menú **Administrar**, haga clic en **Tareas y trabajos**.
2. En el panel izquierdo, haga clic con el botón derecho en la carpeta donde desee crear la tarea y haga clic en **Nueva > Tarea**.
3. En el cuadro de diálogo **Crear una nueva tarea**, en el panel izquierdo, seleccione la tarea que tiene una opción **Opciones avanzadas** (por ejemplo: **Ejecutar archivo de comandos**).
4. En el panel derecho, haga clic en **Opciones avanzadas**.
5. Seleccione **Guardar el resultado de la secuencia de comandos con estado de tarea** y después haga clic en **Aceptar**.

   Cuando este cuadro se selecciona para una tarea, todas las propiedades de tarea están visibles y disponibles para las tareas subsiguientes en un trabajo.
6. Configure la tarea.
7. En el cuadro de diálogo **Crear una nueva tarea**, haga clic en **Aceptar**.

Para crear una tarea que obtenga las propiedades de la entrada de otra tarea

1. En Symantec Management Console, en el menú **Administrar**, haga clic en **Tareas y trabajos**.
2. En el panel izquierdo, haga clic con el botón derecho en la carpeta donde desee crear la tarea y haga clic en **Nueva > Tarea**.
3. En el cuadro de diálogo **Crear una nueva tarea**, en el panel izquierdo, seleccione una tarea de script.

   Las tareas de script reciben propiedades de la entrada.
4. Para usar esta tarea a fin de pasar las propiedades a otra tarea, haga clic en **Opciones avanzadas**, seleccione **Guardar el resultado de la secuencia de comandos con estado de tarea** y después haga clic en **Aceptar**.
5. En el cuadro de diálogo **Crear una nueva tarea**, en la sección de comando script, especifique uno o más tokens (por ejemplo: `%!input!%`) que encuentren la salida.
6. Haga clic en **Aceptar**.

Para configurar tareas en un trabajo de la entrada

1 Cree un trabajo y ponga en él las tareas que creó para la salida y la entrada de información. Cada tarea de salida debe preceder a la tarea que recibe su salida.

Ver "Cómo crear un trabajo" en la página 418.

2 Configure cada tarea de entrada del trabajo.

A la derecha, aparece una entrada de la tarea cuando hace clic en la tarea en las situaciones siguientes: cuando una tarea de cliente tiene entrada y está en un trabajo del cliente, o cuando hay una tarea del cliente dentro de un trabajo del servidor.

Preguntarme por la entrada de la tarea cada vez que se ejecute este trabajo	Selecciónela para escribir la entrada manualmente cuando el trabajo se ejecuta.
Especifique la entrada de la tarea ahora	Selecciónela para escribir la entrada de la tarea en este momento: ■ **Utilizar un valor definido** Selecciónela para usar un valor que no cambie. Escriba el valor en el campo que aparece cuando la pantalla se actualiza. Si esta es una tarea de cliente en un trabajo de servidor, es necesario seleccionar el equipo o los equipos que ejecutan la tarea de cliente. Todas las tareas de cliente tienen este parámetro como parámetro predeterminado de la entrada cuando son trabajos interiores del servidor. ■ **Usar la salida de una tarea anterior** Selecciónela para usar la salida de una tarea anterior. Use este parámetro si hay una tarea de salida en este trabajo que desee usar. Cuando la pantalla se actualiza, el nombre de la variable aparece además de una lista de tareas de salida disponibles. Seleccione la tarea cuya salida desea usar para esta tarea. ■ **Solicitar en tiempo de ejecución** Selecciónela para que se le solicite la entrada de información en el momento de la ejecución.

3 Haga clic en **Aceptar**.

Cómo limpiar datos de tarea

Para disminuir la carga en los recursos del sistema, los datos de tareas se puede archivar o eliminar usando opciones de limpieza.

Ver "Acerca de la administración de tareas " en la página 407.

Ver "Secuenciación de tareas" en la página 416.

Para limpiar datos de tareas

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Todas las configuraciones**.
2. En el panel izquierdo, haga clic en **Notification Server > Configuración de tareas > Datos de la tarea de limpieza**.
3. En la página **Datos de la tarea de limpieza**, edite los detalles necesarios.

   Cada noche, los datos de tareas actuales y los archivados se mueven o son eliminados de acuerdo a la siguiente configuración.

Cantidad máxima de filas en la base de datos en funcionamiento	Cuando el número de filas en uso de la base de datos alcanza la cantidad máxima, las filas más antiguas se guardan hasta que la cantidad máxima no vuelva a excederse. Las filas en uso de la base de datos son aquellas filas que se han usado de forma reciente. Se recomienda mantener un número bajo para disminuir la carga en los recursos del sistema.
Ejecutar tarea de limpieza a petición	Si selecciona esta opción y si el número de filas usadas se excede, la tarea de limpieza se inicia de forma inmediata.

4. (Opcional) Agregue una programación para limpiar los datos de tarea.

   Ver "Adición de una programación a una política, una tarea o un trabajo" en la página 424.
5. Haga clic en **Guardar cambios**.

Limpiar datos de la versión de la tarea

Para disminuir la carga en los recursos del sistema, el historial de versiones de tarea se puede archivar o eliminar usando opciones de limpieza.

Ver "Acerca de la administración de tareas " en la página 407.

Ver "Secuenciación de tareas" en la página 416.

Para limpiar los datos de la versión de la tarea

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Todas las configuraciones**.
2. En el panel izquierdo, haga clic en **Notification Server > Configuración de tareas > Limpiar datos de versión**.
3. En la página **Limpiar datos de versión**, edite los detalles necesarios.

   De forma predeterminada, cada semana, se eliminan las versiones de tarea según la configuración siguiente.

Número máximo de versiones de tarea que se debe conservar en la base de datos	Una vez que el número de versiones alcanza el número seleccionado, se eliminan las más antiguas para mejorar el rendimiento de la base de datos. Es posible seleccionar conservar 1, 5, 10 o 20 versiones de una tarea en la base de datos.

4. (Opcional) Agregue una programación para limpiar los datos de tarea.

   Ver "Adición de una programación a una política, una tarea o un trabajo" en la página 424.
5. Haga clic en **Guardar cambios**.

Cómo cambiar la configuración de Client Task Agent

El Agente de tareas del cliente forma parte de Symantec Management Agent. Recibe trabajos y tareas del servidor de tareas y los ejecuta en equipos administrados. Luego vuelve a informar a Notification Server.

Nota: Cuando instala Symantec Management Agent en un equipo, existe un retraso antes de que Client Task Agent se registre con Notification Server. Cualquier tarea que se realice en el equipo durante este tiempo (aproximadamente 10 minutos) tiene el estado pendiente hasta que Client Task Agent se registre. Cuando se registra Client Task Agent, las tareas se ejecutan de forma inmediata.

Nota: Client Task Agent abre generalmente una conexión directa con Task Server en el puerto 50124. Task Server usa esta conexión para decir al agente cuando las nuevas tareas están disponibles. Sin embargo, si se usa una conexión proxy, no se puede establecer una conexión directa, de modo que Task Server no puede notificar al agente cuando aparecen nuevas tareas disponibles. Para mantener el sistema actualizado, es necesario determinar el valor apropiado en **Comprobar Task Server en busca de nuevas tareas** en el campo **Actualización de tareas**.

Ver "Acerca de la administración de tareas " en la página 407.

Ver "Secuenciación de tareas" en la página 416.

Ver "Componentes de administración de tareas" en la página 409.

Es posible cambiar la configuración de Client Task Agent para mejorar la eficacia del trabajo entre Client Task Agent y Task Server. Para mejorar la eficacia, se puede configurar el intervalo de tiempo durante el cual es necesario que Client Task Agent solicite tareas de Task Server. Es posible definir el método predeterminado por el cual Notification Server selecciona Task Server. Es posible también definir la acción que desea realizar si hay varios Task Servers disponibles en un sitio.

Para cambiar la configuración de Client Task Agent

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Todas las configuraciones**.
2. En el panel izquierdo, haga clic en **Notification Server > Configuración de tarea > Configuración del agente de tareas**.
3. En la página **Configuración del agente de tareas**, edite los detalles necesarios.

Revisar nuevas tareas de Task Server cada	El intervalo, en minutos, en el cual desea que el agente solicite tareas de Task Server.
Cuando varios Task Servers están disponibles en un sitio	La acción que desea realizar si hay varios Task Servers disponibles en un sitio.

4. Seleccione los destinos, los equipos o los usuarios para la aplicación de los cambios.
5. Haga clic en **Guardar cambios**.

Acceder al Portal de trabajos y tareas

El Portal de trabajos y tareas le permite crear y programar tareas para ejecutarlas en sus recursos administrados. Es posible acceder al Portal de trabajos y tareas desde Symantec Management Console.

El Portal de trabajos y tareas le da fácil acceso a la mayoría de las acciones de trabajo y tareas que la Administración de tareas proporciona.

Se proporcionan varios elementos web en esta página:

Inicio rápido - Trabajos y tareas	Permite crear, ejecutar o programar trabajos y tareas.
Task Servers	Permite ver los Task Servers y cuántos equipos cliente están conectados a cada Task Server.
Equipos y dispositivos de tarea	Permite ver los Task Servers y los equipos administrados.

Es posible también configurar la página para que muestre los elementos web que desee. El botón **Editar**, en la esquina superior derecha, permite cambiar los elementos web que se visualizan en este portal.

Para acceder al Portal de trabajos y tareas

1. En **Symantec Management Console**, en el menú **Configuración**, haga clic en **Consola > Páginas del portal**.
2. En el panel izquierdo, haga clic en **Portal de trabajos y tareas**.
3. (Opcional) En el **Portal de trabajos y tareas**, haga clic en el icono **Actualizar** en el elemento web que desee actualizar.

   Si desea configurar una actualización automática para un elemento web, haga clic en el icono **Actualizar**, seleccione **Actualizar cada** y, a continuación, en la lista desplegable, haga clic en el intervalo de actualización que desee.

Capítulo 27

Uso del Administrador de recursos

En este capítulo se incluyen los temas siguientes:

- Acerca de la administración de recursos
- Acceso al Administrador de recursos
- Visualización de datos de inventario para una clase de datos
- Visualización de datos del evento para una clase de datos
- Cómo agregar un recurso a un grupo organizativo
- Tareas del Administrador de recursos

Acerca de la administración de recursos

Es posible administrar los recursos en la Base de datos de la administración de configuración (CMDB) con el Administrador de recursos. El Administrador de recursos permite ver la información y realizar varias tareas en un recurso. La información disponible y las tareas que se pueden realizar dependen del tipo de recurso que se seleccione.

Cuando usted accede a Administrador de recursos, **Página del Portal de recursos básicos** se muestra para todos los recursos excepto los equipos y los paquetes de software. Para un paquete de software o recurso del equipo, aparece la página **Administrador de recursos**. La página que muestra para los recursos que no son del equipo contiene el componente Web part **Resumen de propiedad de elementos**. Este componente Web part muestra la información de las propiedades sobre el recurso seleccionado (tal como GUID y nombre de producto). Para un recurso del equipo, la página muestra una página de resumen para el recurso del

equipo. Si usted hace clic en **Portal de administrador de recursos** en el menú **Inicio**, usted puede acceder al componente Web part **Resumen de propiedad de elementos** para un recurso del equipo.

Ver "Tareas del Administrador de recursos" en la página 437.

Es posible acceder al Administrador de recursos de varias maneras. Los diferentes métodos facilitan el acceso al Administrador de recursos, sin importar donde está en Symantec Management Console.

Ver "Acceso al Administrador de recursos" en la página 434.

Acceso al Administrador de recursos

Es posible acceder al Administrador de recursos de las siguientes maneras:

- Cómo usar el menú **Administrar** en Symantec Management Console
- Haciendo clic con el botón derecho en un recurso, en una lista o en un informe
- Doble clic con el botón derecho en un recurso de una lista o de un informe
- Cómo escribir una URL en el navegador web

Ver "Acerca de la administración de recursos" en la página 433.

Para acceder al Administrador de recursos desde el menú Administrar

1. En Symantec Management Console, en el menú **Administrar**, haga clic en **Recurso**.
2. En el cuadro de diálogo **Seleccionar recurso**, seleccione el recurso que desee administrar y, luego, haga clic en **Aceptar**.

   La página Administrador de recursos se abre con la información de resumen sobre el recurso seleccionado.

Para acceder al Administrador de recursos desde un menú contextual

- En una lista de recursos o un informe dentro de Symantec Management Console, haga clic con el botón derecho en el recurso que desee administrar y haga clic en **Administrador de recursos**.

  En algunas listas, recursos o informes, es posible que la opción del menú contextual del Administrador de recursos no esté disponible. En estos casos, use uno de los otros métodos para acceder al Administrador de recursos.

Para acceder al Administrador de recursos haciendo doble clic en un recurso

- En una lista de recursos o un informe de Symantec Management Console, haga doble clic en recurso que desea administrar.

Para acceder al Administrador de recursos desde una URL

- En una ventana del navegador, escriba la siguiente URL:

  http://*NS Name*/Altiris/Console/Dashboard/DashboardView.aspx?name=*Nombre del recurso de destino*

  Nombre de NS es el nombre del equipo con Notification Server. *Nombre del recurso de destino* puede ser el nombre del recurso, el GUID del recurso o el GUID del elemento. Si omite "?name=*Nombre del recurso de destino*", el Administrador de recursos se abre con el error siguiente:

  ```
  No se suministró el GUID de recurso.
  ```

  Al usar una base de datos con diferenciación entre mayúsculas y minúsculas, se asegura de que el nombre del recurso de destino coincida con el nombre y el caso del recurso en la base de datos de administración de configuración (CMDB).

Visualización de datos de inventario para una clase de datos

Con el Administrador de recursos, se pueden ver los datos del evento para una clase de datos determinada. Los datos del inventario que se visualizan dependen de la clase de datos seleccionada. Generalmente, es posible ver datos de estado y actuales. Cuando corresponda, los datos históricos también están disponibles.

Ver "Acceso al Administrador de recursos" en la página 434.

Para visualizar datos de inventario para una clase de datos

1. En Symantec Management Console, en el menú **Administrar**, haga clic en **Recurso**.
2. En el cuadro de diálogo **Seleccionar recurso**, seleccione el recurso que desee administrar y, luego, haga clic en **Aceptar**.
3. En **Administrador de recursos**, en el menú **Ver**, haga clic en **Inventario**.
4. En el árbol, seleccione la clase de datos en la cual desee ver datos de inventario.
5. En el panel derecho, seleccione la ficha que contiene la información que desea ver.

Visualización de datos del evento para una clase de datos

Con el Administrador de recursos, se pueden ver los datos del evento para una clase de datos determinada. Los datos del evento que se visualizan dependen de la clase de datos seleccionada. Es posible ver generalmente datos de estado y actuales sobre la clase de eventos.

Para visualizar datos del evento para una clase de datos

1. En Symantec Management Console, en el menú **Administrar**, haga clic en **Recurso**.
2. En el cuadro de diálogo **Seleccionar recurso**, seleccione el recurso que desee administrar y, luego, haga clic en **Aceptar**.
3. En **Administrador de recursos**, en el menú **Ver**, haga clic en **Eventos**.

   Ver "Acceso al Administrador de recursos" en la página 434.
4. En el árbol, seleccione la clase de datos en la cual desee ver datos del evento.
5. En el panel derecho, seleccione la ficha que contiene la información que desea ver.

Cómo agregar un recurso a un grupo organizativo

El cuadro de diálogo Agregar grupo organizativo permite agregar el recurso seleccionado a un grupo organizativo. Un recurso puede aparecer solamente una vez en cada vista organizativa.

Para agregar un recurso a un grupo organizativo

1. En Symantec Management Console, en el menú **Administrar**, haga clic en **Recurso**.
2. En el cuadro de diálogo **Seleccionar recurso**, seleccione el recurso que desee administrar y, luego, haga clic en **Aceptar**.
3. En el panel izquierdo del **Administrador de recursos**, haga clic en el vínculo **Agregar grupo organizativo**.
4. En el cuadro de diálogo **Agregar grupo organizativo**, seleccione el grupo organizativo al que desea agregar el recurso.
5. Haga clic en **Aceptar**.

Ver "Tareas del Administrador de recursos" en la página 437.

Tareas del Administrador de recursos

El Administrador de recursos permite realizar varias tareas en un recurso. Estas tareas están disponibles en el menú **Tareas** del Administrador de recursos. Las tareas disponibles dependen del tipo de recurso que se seleccione.

Ver "Acerca de la administración de recursos" en la página 433.

Tabla 27-1 Tareas del Administrador de recursos

Tarea	Descripción
Acceder al portal de administración de tareas	Si la tarea que desee realizar no está enumerada en el panel izquierdo, puede acceder al portal de administración de tareas para encontrar tareas adicionales.
Agregar un recurso a un grupo organizativo	Es posible agregar el recurso seleccionado a un grupo organizativo o moverlo a un nuevo grupo organizativo. Si selecciona un grupo organizativo dentro de una vista organizativa a la cual el recurso aún no pertenece, el recurso se agrega al grupo organizativo. Si elige un grupo organizativo dentro de una vista organizativa a la cual el recurso pertenece, el grupo organizativo nuevamente seleccionado reemplaza al grupo organizativo anterior.
Borrar un recurso	Es posible eliminar el recurso seleccionado de la Base de datos de la administración de configuración (CMDB).
Fusionar recursos duplicados de empresa	(Recursos de la empresa solamente). Si hay dos entradas para una misma empresa, se puede usar esta función para fusionar las entradas.
Efectuar ping en el equipo	Es posible usar la opción **Tarea** del menú **Efectuar ping en el equipo** para establecer una comunicación ping con el equipo seleccionado.
Programar tarea	Es posible usar la opción **Tarea** del menú **Programar tarea** para programar la ejecución de un trabajo o de una tarea.
Ver un resumen organizativo	Es posible ver (**Resúmenes** > **Resumen organizativo**) los grupos organizativos a los cuales pertenece un recurso seleccionado.
Ver calendario	Es posible usar la opción **Calendario** del menú **Ver** para ver la información de la programación de Notification Server. Ver "Visualización del calendario interno de programaciones de Notification Server" en la página 124.

Tarea	Descripción
Ver sucesos	Es posible ver los datos del suceso de una clase de datos, incluida información general sobre la clase de datos y el estado de la clase de datos. Ver "Visualización de datos del evento para una clase de datos" en la página 436.
Ver inventario	Es posible ver los datos del inventario de una clase de datos, incluida información general sobre la clase de datos y el estado de la clase de datos. Ver "Visualización de datos de inventario para una clase de datos " en la página 435.
Ver asociación de recursos	En el panel izquierdo, es posible ver los recursos con los cuales se asocia el recurso seleccionado. Si selecciona el recurso asociado en el panel izquierdo, el Administrador de recursos permite administrar dicho recurso.
Ver detalles de los recursos	Cuando el Administrador de recursos se abre, el panel derecho proporciona los detalles sobre el recurso seleccionado.
Ver las asociaciones de los recursos	Es posible usar la opción **Asociación de recursos** del menú **Ver** para ver la información de la asociación de recursos. La página Asociación de recursos muestra información del tipo de asociación de recursos y de los nombres de los tipos de recursos que se asocian con el recurso seleccionado. Ver "Cómo ver y administrar datos de recursos con informes de Notification Server" en la página 440.

Capítulo 28

Cómo usar los informes de Notification Server

En este capítulo se incluyen los temas siguientes:

- Acerca de los informes de Notification Server
- Cómo ver y administrar datos de recursos con informes de Notification Server

Acerca de los informes de Notification Server

Es posible ver y administrar los datos del recurso mediante los informes de Notification Server. Estos informes le brindan información sobre los equipos administrados y no administrados, y sobre la configuración de Notification Server. Las soluciones instaladas, además, proporcionan informes que brindan información específica de esa solución. Por ejemplo, se pueden usar estos informes para aprender sobre qué eventos y políticas de automatización ejecuta Notification Server y sobre cuánto tiempo demoran.

Los informes se pueden asegurar de modo que solamente los usuarios correspondientes puedan ejecutar un informe. Además, los informes se definen de modo tal que devuelven solamente los datos que el usuario que ejecuta el informe tenga permiso para ver. Por ejemplo, si un gerente ejecuta un informe de sueldo, obtiene solamente los sueldos de sus empleados administrados.

Los informes permiten ver la información de varias maneras. Es posible ver la información en tablas o en gráficos. Además, es posible desglosar elementos específicos de un informe para obtener información adicional.

Ver "Cómo ver y administrar datos de recursos con informes de Notification Server" en la página 440.

Se proporciona una amplia variedad de informes con Notification Server. No es posible modificar estos informes predeterminados, pero sí es posible clonarlos y

editar el clon según los requisitos de cada uno. También es posible crear nuevos informes personalizados.

Cómo ver y administrar datos de recursos con informes de Notification Server

Es posible usar los informes para ver y administrar los datos del recurso. Los informes recuperan los datos de la CMDB.

Ver "Acerca de los informes de Notification Server" en la página 439.

Tabla 28-1 Proceso para ver y administrar datos de recursos con informes de Notification Server

Paso	Acción	Descripción
Paso 1	Extraer los resultados del informe.	Es necesario que seleccione el informe que desea usar y, opcionalmente, que establezca los parámetros de usuario y seleccione la instantánea que desea usar. Ver "Cómo extraer resultados del informe de Notification Server" en la página 441.
Paso 2	Ver los resultados del informe.	Puede configurar la vista de informe de manera que se adapte a sus necesidades, así: ■ Seleccione la vista de cuadrícula o la vista de gráfico que desee usar, si se ha instalado alguna otra vista adicional para el informe. ■ Agrupe y ordene las columnas en la vista de cuadrícula. ■ Visualice los resultados en una vista de gráfico, si se ha configurado ese tipo de vista en el informe. Ver "Cómo ver los resultados del informe de Notification Server" en la página 443.

Paso	Acción	Descripción
Paso 3	(Opcional) Usar los resultados del informe.	Es posible usar los resultados del informe de cualquiera de las siguientes maneras: ■ Examine los elementos seleccionados para obtener más información detallada. Al explorar los niveles inferiores de un elemento, se abre la vista correspondiente, que puede ser otro informe o la Consola del administrador de recursos. ■ Realice las acciones en los elementos seleccionados. ■ Imprima los resultados del informe. Ver "Cómo usar los resultados del informe de Notification Server" en la página 444.
Paso 4	(Opcional) Guardar los resultados del informe.	Es posible guardar los resultados del informe en los siguientes formatos: ■ Archivo Se proporcionan con Notification Server los siguientes tipos de archivos: hojas de cálculo (.csv), archivos HTML y archivos XML. Las soluciones instaladas pueden proporcionar opciones para tipos de archivo adicionales. Ver "Cómo guardar los resultados del informe de Notification Server como un archivo" en la página 446. ■ Filtro estático Ver "Cómo crear un filtro estático a partir de resultados del informe de Notification Server" en la página 447. ■ Instantánea Ver "Cómo guardar los resultados del informe de Notification Server como una instantánea" en la página 448. ■ Elemento web Ver "Cómo guardar los resultados del informe de Notification Server como un elemento web" en la página 448.

Cómo extraer resultados del informe de Notification Server

Se proporciona un conjunto de informes con Notification Server y las soluciones instaladas pueden agregar otros informes.

Algunos informes tienen parámetros de usuario que se pueden establecer cuando se extraen los resultados del informe. Los parámetros de usuario son variables en la consulta del informe y hacen que los informes sean más flexibles y eficaces. Por ejemplo, el informe Lista de equipos por tipo de sistema y nombre de SO tiene parámetros de usuario definidos tanto para el tipo de sistema como para el nombre de SO. Cuando se extraen los resultados del informe, se puede especificar la

combinación del tipo y el nombre del sistema operativo que desee usar mediante la configuración de los parámetros correspondientes. Sin parámetros de usuario, cada informe tendría valores fijos definidos dentro de la consulta. Necesitaría tener un informe diferente para cada combinación de tipo y nombre de sistema operativo. Alternativamente, se necesitaría modificar la consulta del informe cada vez que desee extraer resultados.

Para reducir al mínimo la carga en Notification Server, los informes grandes o frecuentemente usados, en general, se programan para ejecutarse en los intervalos correspondientes y se guardan como instantáneas. La creación de instantáneas permite que el resto de los usuarios vea los resultados del informe en la última instantánea en lugar de que cada usuario tenga que ejecutar el informe de nuevo. Los informes programados se ejecutan normalmente con el ámbito de administrador para garantizar que todos los datos disponibles estén incluidos. Cuando se ve el conjunto de resultados del informe, los datos de la instantánea se definen según corresponde. Cuando se ven resultados del informe, se puede elegir una instantánea para usar. Si no elige una instantánea, los resultados se extraen mediante la ejecución de una consulta del informe en CMDB.

En entornos grandes, Symantec recomienda usar la funcionalidad **SuppressReportAutorun**. Cuando se habilita **SuppressReportAutorun** y se abre cualquier informe, el informe no se ejecuta de forma inmediata. Para ver los resultados del informe, es necesario hacer clic en **Actualizar**. Tenga en cuenta que de forma predeterminada la funcionalidad **SuppressReportAutorun** está deshabilitada. Es posible habilitarla en **Configurador de NS**, en **Configuración básica > Interfaz de usuario > Informe > SuppressReportAutorun**.

Ver "Cómo configurar los valores de Notification Server con el configurador de NS" en la página 75.

Esta tarea es un paso en el proceso para ver y administrar los datos de recursos con los informes de Notification Server.

Ver "Cómo ver y administrar datos de recursos con informes de Notification Server" en la página 440.

Para extraer resultados del informe de Notification Server

1. En Symantec Management Console, en el menú **Informes**, haga clic en **Todos los informes**.
2. En el panel izquierdo, seleccione el informe que desea usar.

3 (Opcional) En el panel derecho, en **Parámetros**, establezca los parámetros de usuario apropiados.

Ver "Definir parámetros y proveedores de valores para un informe personalizado" en la página 460.

4 Si desea usar una instantánea, en la lista desplegable **Ver**, seleccione la instantánea correspondiente.

Las opciones que se han predefinido son:

- Actual
- Instantánea más reciente

Se enumera cualquier instantánea adicional que se haya creado. Cada una tiene una etiqueta con su fecha y hora de creación.

Cómo ver los resultados del informe de Notification Server

Es posible visualizar los resultados del informe mediante las siguientes vistas, si estas se han configurado para el informe:

Vista de cuadrícula	Las vistas de cuadrícula son tablas, con cada elemento del resultado visualizado en una fila diferente. Las columnas disponibles se definen en el informe. Es posible cambiar el orden de las columnas y agrupar los resultados según los valores en una columna determinada. Por ejemplo, es posible que desee agrupar una lista de equipos por el tipo o la subred del sistema operativo.
Vista de gráficos	Las vistas de gráfico son formatos gráficos, como gráficos de barras, gráficos lineales, gráficos circulares y gráficos de área. Se pueden definir varias vistas de gráfico en el informe, pero se puede ver solamente una por vez.

Cada gráfico o cuadrícula es una vista determinada en los resultados del informe, de modo que una vista puede contener un subconjunto de resultados. Un informe puede tener varias vistas disponibles para personalizar la salida para los diferentes usuarios en lugar de tener que crear diferentes informes para cada usuario. Por ejemplo, un informe que enumera los equipos administrados puede incluir las propiedades de cada equipo, como el sistema operativo, el tipo de procesador y el tamaño del disco. El informe puede tener varias vistas diferentes y cada vista puede contener un subconjunto de las propiedades disponibles para cada equipo. Cuando se mira el informe, se puede elegir la vista que contiene las propiedades que le interesan.

Cuando se guarda un informe, se guardan todos los resultados que están en su ámbito. No se limita a los datos que se visualizan en la vista actual. Cuando se imprime un informe, se imprime la vista actual.

Esta tarea es un paso en el proceso para ver y administrar los datos de recursos con los informes de Notification Server.

Ver "Cómo ver y administrar datos de recursos con informes de Notification Server" en la página 440.

Para ver los resultados del informe de Notification Server

1. En Symantec Management Console, en el menú **Informes**, haga clic en **Todos los informes**.
2. En el panel izquierdo, seleccione el informe que desea usar.
3. En el panel derecho, en la lista desplegable **Ver**, seleccione la vista apropiada.

   Las vistas de cuadrícula y de gráfico que se crearon están incluidas en una lista.
4. (Opcional) Si desea agrupar los resultados, seleccione la columna correspondiente de la lista desplegable **Agrupar por**.
5. (Opcional) Si desea cambiar el orden de las columnas, haga clic en el encabezado de una columna y arrástrela a la posición apropiada.

Cómo usar los resultados del informe de Notification Server

Es posible explorar los niveles inferiores de los resultados del informe para obtener información adicional. Al explorar los niveles inferiores de un elemento, se abre la vista correspondiente, que puede ser otro informe o el administrador de recursos.

Es posible realizar acciones en recursos directamente desde los resultados del informe. Por ejemplo, se puede ejecutar un informe que enumere todos los equipos que cumplen criterios específicos. Es posible luego realizar una acción en algunos de los equipos o en todos. Las acciones disponibles son las que se aplican al tipo de recurso seleccionado y que tiene permiso para realizar.

Es posible imprimir filas seleccionadas de resultados o todos los resultados del informe.

Esta tarea es un paso en el proceso para ver y administrar los datos de recursos con los informes de Notification Server.

Ver "Cómo ver y administrar datos de recursos con informes de Notification Server" en la página 440.

Para explorar los niveles inferiores de los resultados del informe

1. En Symantec Management Console, en el menú **Informes**, haga clic en **Todos los informes**.
2. En el panel izquierdo, seleccione el informe que desea usar.
3. En el panel derecho, en la lista desplegable **Ver**, seleccione la vista apropiada.
4. En los resultados del informe, haga clic en el elemento para el cual desee obtener información adicional.

   Tenga en cuenta que la acción de examinar de niveles inferiores puede variar: puede ser un solo clic o un doble clic.

Para realizar acciones en los recursos enumerados en los resultados del informe

1. En los resultados del informe, seleccione los recursos en los cuales desee realizar una acción.
2. Haga clic en **Acciones** y después seleccione la opción apropiada.

   Tenga en cuenta que esta función no está siempre disponible.

Para imprimir los resultados del informe

1. Si es necesario, en los resultados del informe, seleccione las filas de los resultados del informe que desee imprimir.
2. Haga clic en **Imprimir**.
3. En el cuadro de diálogo **Imprimir**, especifique las siguientes opciones:

Parámetros	Si desea incluir la configuración de parámetros del usuario en los resultados impresos, seleccione **Incluir parámetros**.
Rango de datos	Elija alguna de las siguientes opciones: ■ Imprimir todo: incluye todos los resultados del informe. ■ Imprimir filas seleccionadas: incluye solamente las filas seleccionadas de los resultados del informe.

4. Haga clic en **Imprimir**.

   Se muestra una vista previa de la impresión del informe en una nueva ventana del navegador, y aparece el cuadro de diálogo Impresión de Windows. La vista previa es igual a la que se ve cuando se guarda el informe como HTML.
5. En el cuadro de diálogo **Impresión de Windows**, seleccione las opciones apropiadas y después haga clic en **Imprimir**.

Cómo guardar los resultados del informe de Notification Server como un archivo

Es posible guardar los resultados del informe como un archivo. Es posible guardar todos los resultados o se pueden seleccionar los resultados que desee incluir. Se proporcionan con Notification Server opciones para archivos de hojas de cálculo (.csv), HTML y XML. Las soluciones instaladas pueden proporcionar opciones para tipos de archivo adicionales.

Esta tarea es un paso en el proceso para ver y administrar los datos de recursos con los informes de Notification Server.

Ver "Cómo ver y administrar datos de recursos con informes de Notification Server" en la página 440.

Para guardar los resultados del informe de Notification Server como un archivo

1. En Symantec Management Console, en el menú **Informes**, haga clic en **Todos los informes**.
2. En el panel izquierdo, seleccione el informe que desea usar.
3. (Opcional) En el panel derecho, seleccione las filas de los resultados del informe que desee incluir en el archivo.
4. Haga clic en **Guardar como** y después haga clic en el tipo de archivo apropiado.
5. En el cuadro de diálogo **Guardar como**, especifique las siguientes opciones:

Parámetros	Si desea incluir la configuración de parámetros del usuario en el archivo, seleccione **Incluir parámetros**.
Rango de datos	Elija alguna de las siguientes opciones: ■ Guardar todo: incluye todos los resultados del informe en el filtro. ■ Guardar filas seleccionadas: incluye solamente las filas seleccionadas de los resultados del informe en el filtro.

6. Haga clic en **Guardar**.
7. En el cuadro de diálogo **Guardar informe**, seleccione la carpeta en la cual desea guardar el archivo y después haga clic en **Guardar**.

Cómo crear un filtro estático a partir de resultados del informe de Notification Server

Es posible crear un nuevo filtro estático guardando los resultados de un informe. Puede incluir todos los resultados o puede seleccionar los resultados que desee incluir.

Ver "Acerca de los filtros de recursos" en la página 353.

Esta tarea es un paso en el proceso para ver y administrar los datos de recursos con los informes de Notification Server.

Ver "Cómo ver y administrar datos de recursos con informes de Notification Server" en la página 440.

Para crear un filtro estático de resultados del informe de Notification Server

1. En Symantec Management Console, en el menú **Informes**, haga clic en **Todos los informes**.
2. En el panel izquierdo, seleccione el informe que desea usar.
3. (Opcional) En el panel derecho, seleccione las filas de los resultados del informe que desee incluir en el filtro.
4. Haga clic en **Guardar como > Filtro estático**.
5. En el cuadro de diálogo **Guardar como filtro estático**, especifique las opciones apropiadas:

Nombre	El valor predeterminado es el nombre del informe. Si desea cambiar el nombre, escriba el nombre apropiado del filtro.
Seleccione un recurso en el que se basará el filtro	Esta opción se aplica a los informes de recursos solamente. En la lista desplegable, seleccione la opción apropiada.
Rango de datos	Elija alguna de las siguientes opciones: ■ Guardar todo: incluye todos los resultados del informe en el filtro. ■ Guardar filas seleccionadas: incluye solamente las filas seleccionadas de los resultados del informe en el filtro.

6. Haga clic en **Guardar**.

   El filtro nuevo se almacena en el árbol Filtros, en la carpeta Filtros basados en informes.

Cómo guardar los resultados del informe de Notification Server como una instantánea

Es posible guardar los resultados actuales del informe como una instantánea. Por ejemplo, es posible que desee guardar un conjunto determinado de resultados y ponerlos a disposición de otros usuarios sin volver a extraerlos de la CMDB. Cuando guarda un informe como instantánea, se guarda según su alcance. Solamente los usuarios que comparten el mismo rol de seguridad pueden ver la instantánea.

Esta tarea es un paso en el proceso para ver y administrar los datos de recursos con los informes de Notification Server.

Ver "Cómo ver y administrar datos de recursos con informes de Notification Server" en la página 440.

Para guardar los resultados del informe de Notification Server como una instantánea

1. En Symantec Management Console, en el menú **Informes**, haga clic en **Todos los informes**.
2. En el panel izquierdo, seleccione el informe que desea usar.
3. En el panel derecho, haga clic en **Guardar como > Instantánea**.

   La nueva instantánea estará disponible en la lista desplegable **Ver** la próxima vez que abra el informe.

Cómo guardar los resultados del informe de Notification Server como un elemento web

Es posible guardar un informe como un elemento web que se puede usar en la página de un portal. El informe del elemento web es una copia del informe que es dinámica y completamente funcional. El conjunto de resultados que se muestra en la página del portal se actualiza cuando se abre la página, de forma que siempre está actualizado. El informe del elemento web es independiente del informe original y, por lo tanto, los cambios que se realizan en un informe no se propagan al otro.

Ver "Creación y modificación de elementos web" en la página 61.

Esta tarea es un paso en el proceso para ver y administrar los datos de recursos con los informes de Notification Server.

Ver "Cómo ver y administrar datos de recursos con informes de Notification Server" en la página 440.

Para guardar los resultados del informe de Notification Server como un elemento web

1. En Symantec Management Console, en el menú **Informes**, haga clic en **Todos los informes**.
2. En el panel izquierdo, seleccione el informe que desea usar.
3. En el panel derecho, haga clic en **Guardar como > Elemento web**.
4. (Opcional) En el cuadro de diálogo **Guardar como elemento web**, edite el nombre del nuevo elemento web.

   El nombre predeterminado debe ser adecuado para la mayoría de los propósitos.
5. (Opcional) En la lista desplegable **Seleccionar un tamaño de elemento web**, seleccione el tamaño apropiado.

   La opción predeterminada es Pequeño.
6. Haga clic en **Guardar**.

   El nuevo elemento web se guarda en la carpeta Settings\Console Settings\Webparts.

Capítulo 29

Cómo crear los informes personalizados de Notification Server

En este capítulo se incluyen los temas siguientes:

- Componentes de un informe personalizado de Notification Server
- Creación y modificación de informes personalizados de Notification Server

Componentes de un informe personalizado de Notification Server

Los informes de Notification Server se construyen a partir de un conjunto estándar de componentes.

Tabla 29-1 Componentes de un informe personalizado de Notification Server

Componente	Descripción
Origen de datos	El origen de datos es el componente que proporciona los datos del informe. Los informes personalizados y los filtros dinámicos usan las consultas SQL que se ejecutan en la CMDB para extraer los datos apropiados. Las soluciones pueden proporcionar informes que usan otros orígenes de datos, como hojas de cálculo o archivos CSV. Los informes personalizados y los filtros dinámicos usan una consulta SQL como origen de datos. Es posible definir la consulta escribiendo el código SQL desde el comienzo o usando la Generación de consultas. Ver "Cómo definir una consulta de recursos para un informe personalizado" en la página 457. Ver "Cómo definir una consulta SQL para un informe personalizado" en la página 459.
Vistas	Una vista de informe es una manera determinada en la que se visualizan los datos del informe. Una visión contiene por lo general un subconjunto de los datos del informe. Los datos se presentan de una manera que sea apropiada para un rol de usuario determinado. Es posible elegir las columnas de datos que se incluirán en la vista y especificar cuál se debe usar como el eje principal. Los tipos de vistas disponibles son: ■ Vista de cuadrícula Vea los datos de informes en formato tabular, con cada elemento visualizado en una fila separada. ■ Vista de gráficos Vea los datos de informes en formato gráfico, como gráficos de barras, gráficos de líneas, gráficos circulares y gráficos de área. ■ Texto con plantillas La configuración de un número de vistas distintas para un informe le permite personalizar los datos del informe para diferentes usuarios. Es posible usar un único informe para todos los usuarios, en lugar de crear varios informes para cumplir los requisitos de diferentes usuarios. Ver "Cómo crear o modificar una vista de gráfico para un informe personalizado" en la página 462. Ver "Cómo crear o modificar una vista de cuadrícula para un informe personalizado" en la página 464.

Componente	Descripción
Parámetros	Los parámetros son variables en la consulta de informe que el usuario puede configurar cuando ejecuta el informe. El uso de parámetros genera informes más flexibles y eficaces. Por ejemplo, el informe Lista de equipos por tipo de sistema y nombre de SO tiene parámetros de usuario definidos tanto para el tipo de sistema como para el nombre de SO. Cuando se ejecuta este informe, se puede especificar la combinación del tipo y el nombre del sistema operativo que desee usar mediante la configuración de los parámetros correspondientes. Sin parámetros, cada informe tendría valores fijos definidos dentro de la consulta. Ver "Definir parámetros y proveedores de valores para un informe personalizado" en la página 460.
Exploraciones de niveles inferiores	El examen de niveles inferiores de un informe es una acción que se realiza cuando el usuario hace clic en un elemento en los resultados del informe. Es posible agregar exploraciones de niveles inferiores en un informe para permitir al usuario obtener información adicional a través de los resultados del informe. Para cada examen de niveles inferiores, se puede especificar la vista en la cual la exploración está disponible y cómo el usuario activa el examen de niveles inferiores. Es posible también especificar la acción que se realiza y los parámetros que se usarán en la acción. Es posible configurar varias exploraciones de niveles inferiores en un informe para realizar diferentes acciones en diferentes tipos de recursos. Ver "Cómo configurar acciones de examinación de niveles inferiores para un informe personalizado" en la página 465.

Creación y modificación de informes personalizados de Notification Server

Los informes de Notification Server permiten ver y administrar los datos del recurso. Estos informes brindan información sobre los equipos administrados y no administrados, y sobre la configuración de Notification Server. Symantec Management Platform incluye una amplia gama de informes. Además, permite crear informes personalizados a fin de satisfacer las necesidades de la organización. Los informes de Notification Server recuperan los datos de la base de datos de administración de configuración (CMDB).

Los datos del informe se pueden usar de las siguientes maneras:

- El origen de datos de una política de automatización.

- Un elemento web que visualiza los datos actuales en una página del portal.
- Un informe del recurso que permite al usuario examinar un recurso determinado a fin de ver todos los detalles en el Administrador de recursos.
- Un informe de tendencia que muestra los cambios de los datos a lo largo del tiempo.
- Varios informes de examen de niveles inferiores (por ejemplo, informes de jerarquía) que permiten al usuario explorar datos de nivel superior para ver datos de nivel inferior más detallados.

Para crear o modificar un informe personalizado, es necesario definir los componentes del informe en la página **Edición de informes personalizada**.

Ver "Página Edición de informes personalizada" en la página 526.

Ver "Componentes de un informe personalizado de Notification Server" en la página 450.

Nota: Algunas políticas de automatización usan un informe como origen de datos y pueden depender de algunos resultados o parámetros determinados. Cuando se modifica un informe, debe asegurarse de que los cambios no afecten ninguna política de automatización.

Ver "Especificación del origen de datos de políticas de automatización" en la página 401.

Tabla 29-2 Proceso para crear y modificar informes personalizados de Notification Server

Paso	Acción	Descripción
Paso 1	Cree un nuevo informe o seleccione un informe existente para modificar.	Cree un nuevo informe desde el comienzo o clone un informe predeterminado que se proporcione con Notification Server. Es posible modificar cualquier informe personalizado que se haya creado, pero no puede modificar los informes predeterminados. Ver "Cómo crear un informe personalizado de Notification Server" en la página 455. Ver "Cómo modificar un informe personalizado existente de Notification Server" en la página 456.

Paso	Acción	Descripción
Paso 2	Cree la consulta de informe.	Puede escribir la consulta SQL usted mismo o usar la Generación de consultas para generar la consulta de informe. La Generación de consultas es una herramienta fácil de usar que le permite seleccionar las tablas y los campos que desea usar. Ver "Cómo definir una consulta de recursos para un informe personalizado" en la página 457. También puede escribir el código SQL desde el comienzo. Como alternativa, puede copiar el código SQL de otro filtro o informe y modificarlo para que se adapte a sus requisitos. Ver "Cómo definir una consulta SQL para un informe personalizado" en la página 459.
Paso 3	Especifique los proveedores de valores para los parámetros.	Si la consulta de informe incluye parámetros, puede definir los proveedores de valores correspondientes. El proveedor de valores permite al usuario configurar el valor apropiado para el parámetro de la consulta cuando ejecutan el informe. Ver "Definir parámetros y proveedores de valores para un informe personalizado" en la página 460.
Paso 4	Cree las vistas de informe.	Una vista de informe contiene por lo general un subconjunto de resultados del informe. Los resultados se presentan de una manera que sea apropiada para un rol de usuario determinado. La configuración de un número de vistas distintas para un informe le permite personalizar los resultados del informe para diferentes usuarios. Ver "Cómo crear o modificar una vista de gráfico para un informe personalizado" en la página 462. Ver "Cómo crear o modificar una vista de cuadrícula para un informe personalizado" en la página 464.
Paso 5	Cree las exploraciones de niveles inferiores.	El examen de niveles inferiores de un informe es una acción que se realiza cuando el usuario hace clic en un elemento en los resultados del informe. Es posible configurar exploraciones de niveles inferiores en un informe para permitir al usuario obtener información adicional a través de los resultados del informe. Ver "Cómo configurar acciones de examinación de niveles inferiores para un informe personalizado" en la página 465.

Paso	Acción	Descripción
Paso 6	Especifique las propiedades del informe.	Es posible elegir si los resultados del informe están restringidos por el ámbito del usuario que ejecuta el informe. Es posible también ejecutar el informe solamente como una instantánea. Para reducir al mínimo la carga en Notification Server, se recomienda ejecutar los informes grandes o usados frecuentemente como instantáneas. Ver "Cómo especificar las propiedades avanzadas de un informe personalizado" en la página 468.
Paso 7	Guarde el informe.	Guarde los cambios en el nuevo informe o el informe modificado. Ver "Cómo crear un informe personalizado de Notification Server" en la página 455. Ver "Cómo modificar un informe personalizado existente de Notification Server" en la página 456.

Cómo crear un informe personalizado de Notification Server

Es posible crear sus propios informes personalizados y configurarlos para satisfacer sus requisitos. Es posible crear un nuevo informe desde el comienzo, o bien clonar un informe predeterminado que se proporcione con Notification Server.

Esta tarea es un paso en el proceso para crear y modificar los informes personalizados de Notification Server.

Ver "Creación y modificación de informes personalizados de Notification Server" en la página 452.

Para crear un informe personalizado de Notification Server

1. En Symantec Management Console, en el menú **Informes**, haga clic en **Todos los informes**.
2. En el panel izquierdo, haga clic con el botón derecho en la carpeta en la que desea agregar el nuevo informe y, a continuación, haga clic en **Nuevo > Informe**.

3 Haga clic en alguna de las siguientes opciones:

Informe de equipo	La consulta de informe es una consulta de recurso, y la plantilla base selecciona todos los equipos. Es posible restringir la consulta para seleccionar los equipos que desee.
Informe de usuario	La consulta de informe es una consulta de recurso, y la plantilla base selecciona todos los usuarios. Es posible restringir la consulta para seleccionar los usuarios que desee.
Informe del recurso	La consulta de informe es una consulta de recurso, y la plantilla base selecciona todos los recursos (incluidos todos los equipos y todos los usuarios). Es posible restringir la consulta para seleccionar los recursos que desee.
Informe de SQL	La consulta de informe es una consulta SQL. Es posible escribir su propia consulta SQL para extraer los datos que desee de la CMDB. No se aplica ninguna plantilla, y no hay restricciones con respecto a lo que se puede escribir.

4 (Opcional) En el panel derecho, especifique el nombre del informe y la descripción.

5 En la página Edición de informes personalizada, especifique los componentes del informe e informe las propiedades en las fichas apropiadas.

Ver "Página Edición de informes personalizada" en la página 526.

Para obtener más información, haga clic en la página y, después, presione **F1**.

6 Para guardar los cambios sin salir del modo de edición, haga clic en **Aplicar**.

7 Para obtener una vista previa de los cambios sin salir del modo de edición, haga clic en **Vista previa**.

8 Para guardar los cambios y salir del modo de edición, haga clic en **Guardar cambios**.

Cómo modificar un informe personalizado existente de Notification Server

Es posible modificar sus propios informes personalizados en cualquier momento. Sin embargo, no es posible modificar los informes predeterminados que se

proporcionan con Notification Server. Si desea modificar un informe predeterminado, se puede clonar el informe para crear una copia de él y después editar la copia.

Esta tarea es un paso en el proceso para crear y modificar los informes personalizados de Notification Server.

Ver "Creación y modificación de informes personalizados de Notification Server" en la página 452.

Para modificar un informe personalizado existente de Notification Server

1. En Symantec Management Console, en el menú **Informes**, haga clic en **Todos los informes**.
2. En el panel izquierdo, haga clic en el informe que desea modificar.
3. En el panel derecho, en la esquina derecha, haga clic en **Editar**.
4. (Opcional) Modifique el nombre y la descripción del informe.
5. En la página **Edición de informes personalizada**, realice sus cambios a los componentes del informe e informe las propiedades en las fichas apropiadas.

   Ver "Página Edición de informes personalizada" en la página 526.

   Para obtener más información, haga clic en la página y, después, presione **F1**.
6. Para guardar los cambios sin salir del modo de edición, haga clic en **Aplicar**.
7. Para obtener una vista previa de los cambios sin salir del modo de edición, haga clic en **Vista previa**.
8. Para guardar los cambios y salir del modo de edición, haga clic en **Guardar cambios**.

Cómo definir una consulta de recursos para un informe personalizado

Cuando crea o modifica su propio informe personalizado de Notification Server, se puede definir una consulta del informe. Para obtener un informe del equipo, del usuario o del recurso, es necesario definir una consulta de recursos.

Una consulta de recursos se basa en las tablas que están disponibles en la base de datos de administración de configuración (CMDB). La Generación de consultas es una herramienta fácil de usar que proporciona una plantilla estándar y le permite seleccionar las tablas y los campos que desea usar. Lo ayuda a definir la consulta para que se adapte a sus requisitos. No necesita ningún conocimiento sobre SQL para definir una consulta de recurso. La consulta de recurso se convierte en SQL automáticamente, y SQL se ejecuta en la CMDB para extraer los recursos apropiados.

Cuando haya definido una consulta de recursos para su informe personalizado, podrá convertir una consulta de recursos en la consulta SQL equivalente. Por ejemplo, puede usar el Generador de consultas para definir la estructura de la consulta, convertirla en SQL y modificar el SQL directamente. Este proceso puede ser más rápido y más eficaz que escribir toda la consulta en SQL desde el comienzo.

Cuando se crea un nuevo informe del equipo, del usuario o del recurso, una plantilla de consulta de recurso se agrega al informe automáticamente. Cuando se crea un nuevo filtro, la misma plantilla de consulta de recurso se agrega al filtro cuando se elige el modo de consulta Generación de consultas. La consulta base de la plantilla selecciona todos los equipos, usuarios o recursos, correspondientes al tipo de informe. Se debe modificar la consulta base para seleccionar los recursos apropiados.

Esta tarea es un paso en el proceso para crear y modificar los informes personalizados de Notification Server.

Ver "Creación y modificación de informes personalizados de Notification Server" en la página 452.

Para definir una consulta de recursos para un informe personalizado

1. En Symantec Management Console, en el menú **Informes**, haga clic en **Todos los informes**.
2. Realice una de las siguientes acciones:
   - Para definir una consulta de recursos para un nuevo informe que se crea, en el panel izquierdo, haga clic con el botón derecho en la carpeta en la cual desea agregar el nuevo informe. Haga clic en **Nuevo** y en **Informe de equipo**, **Informe de usuario** o **Informe del recurso**.
   - Para redefinir una consulta de recursos para un informe existente, en el panel izquierdo, haga clic en el informe de equipo, el informe de usuario o el informe de recurso que desee modificar. En el panel derecho, en la esquina superior derecha, haga clic en **Editar**.
3. En el panel derecho, en la ficha **Origen de datos**, especifique los detalles de la consulta.

   Ver "Página Edición de informes personalizada: Ficha Origen de datos " en la página 527.

   Para obtener más información, haga clic en la página y después presione **F1**.

4 (Opcional) Para convertir la consulta de recursos en la consulta SQL equivalente, haga clic en **Convertir esta consulta en una Consulta SQL**.

Advertencia: Convertir una consulta de recurso en una consulta SQL es una operación unidireccional. No es posible convertir de nuevo la consulta SQL resultante en una consulta de recurso.

---

5 Haga clic en **Guardar cambios**.

Cómo definir una consulta SQL para un informe personalizado

Cuando crea o modifica su propio informe personalizado de Notification Server, se puede definir una consulta del informe. Para obtener un informe del equipo, del usuario o del recurso, es necesario definir una consulta de recursos para el informe. Para obtener un informe SQL, es necesario definir una consulta SQL.

Es posible escribir una consulta SQL para definir los recursos que desea incluir en el informe o el filtro. Es posible escribir el código SQL desde el comienzo. Como alternativa, puede copiar el código SQL de otro filtro o informe y modificarlo para que se adapte a sus requisitos. Por ejemplo, se puede crear una consulta de recursos con la Generación de consultas y después copiar el código SQL generado de la ficha Consulta resuelta. También puede usar el Generador de consultas para definir la estructura de la consulta, convertirla en SQL y modificar el SQL directamente.

Cuando se crea un nuevo informe SQL, una plantilla de consulta SQL se agrega al informe automáticamente. Cuando se crea un nuevo filtro, la misma plantilla de consulta SQL se agrega al filtro cuando se elige el modo de consulta SQL sin formato. La consulta SQL base selecciona todos los recursos disponibles. Se debe modificar la consulta base para seleccionar los recursos apropiados.

Se necesita el privilegio de edición de SQL para crear o modificar consultas SQL. También es necesario tener una buena comprensión de la estructura de tablas de la CMDB. Si desea aplicar alguna determinación del ámbito a los resultados de la consulta, es necesario incluir el código SQL apropiado en la consulta.

Esta tarea es un paso en el proceso para crear y modificar los informes personalizados de Notification Server.

Ver "Creación y modificación de informes personalizados de Notification Server" en la página 452.

Para definir una consulta SQL para un informe personalizado

1. En Symantec Management Console, en el menú **Informes**, haga clic en **Todos los informes**.
2. Realice una de las siguientes acciones:
   - Para definir una consulta SQL para un nuevo informe que se crea, en el panel izquierdo, haga clic con el botón derecho en la carpeta en la cual desea agregar el nuevo informe. Haga clic en **Nuevo** y en **Informe de SQL**.
   - Para redefinir una consulta SQL para un informe existente, en el panel izquierdo, haga clic en el informe de SQL que desee modificar. En el panel derecho, en la esquina superior derecha, haga clic en **Editar**.
3. En el panel derecho, en la ficha **Origen de datos**, especifique los detalles de la consulta en las fichas apropiadas.

   Ver "Página Edición de informes personalizada: Ficha Origen de datos " en la página 527.

   Para obtener más información, haga clic en la página y, después, presione **F1**.
4. Haga clic en **Guardar cambios**.

Definir parámetros y proveedores de valores para un informe personalizado

Si la consulta del informe personalizado que crea o modifica incluye parámetros, puede definir los proveedores de valores apropiados. El proveedor de valores de un parámetro permite al usuario configurar el valor apropiado para el parámetro cuando se ejecuta un informe. Incluir en una consulta de informe los parámetros que el usuario puede definir permite crear un único informe flexible que puede extraer diferentes conjuntos de resultados al cambiar los valores del parámetro. La alternativa sería especificar en código los valores del parámetro en la consulta. Luego, se debe modificar la consulta cada vez que desee usar un valor de parámetro diferente. Se pueden además crear varios informes con un valor diferente definido en cada consulta.

El proveedor de valores especifica cómo se configura el valor del parámetro cuando el usuario ejecuta el informe. En muchos casos, el proveedor de valores es un componente de la interfaz de usuario que acepta un valor o una configuración del usuario. Por ejemplo, se puede definir un parámetro como una lista desplegable con un conjunto de valores válidos entre los cuales el usuario puede elegir. Como alternativa, se lo puede definir como un campo de texto que acepta una cadena de caracteres que escribe el usuario. En algunos casos, un parámetro no requiere

un proveedor de valores. El valor del parámetro se configura automáticamente sin la intervención del usuario.

Esta tarea es un paso en el proceso para crear y modificar los informes personalizados de Notification Server.

Ver "Creación y modificación de informes personalizados de Notification Server" en la página 452.

Para agregar un parámetro a un informe personalizado

1. En Symantec Management Console, en el menú **Informes**, haga clic en **Todos los informes**.
2. En el panel izquierdo, seleccione el informe que desee modificar.
3. En la página *Nombre del informe*, en la esquina superior derecha, haga clic en **Editar**.
4. En la ficha **Parámetros de informe**, haga lo siguiente:

Para agregar un parámetro	Haga clic en **Agregar** y, después, haga clic en el parámetro apropiado de la consulta. La lista desplegable contiene todos los parámetros que se definieron en la consulta de informe, pero que aún no se agregaron al informe.
Para agregar un parámetro de tipo avanzado	Haga clic en **Agregar > Tipos avanzados** y, después, haga clic en el tipo que desee.
Para crear un nuevo parámetro	■ Haga clic en **Agregar > Nuevo parámetro**. ■ En el cuadro de diálogo **Edición de parámetro**, en **Parámetro**, especifique la configuración apropiada del parámetro. ■ En **Proveedor de valores**, en la lista desplegable **Nombre**, seleccione el tipo de proveedor de valores que desee usar. ■ En **Configuración**, especifique la configuración apropiada del proveedor de valores. ■ Haga clic en **Aceptar**.

Para modificar un parámetro

- Haga clic en el parámetro que desee modificar y, después, haga clic en el símbolo **Editar**.
- En el cuadro de diálogo **Edición de parámetro**, en **Parámetro**, especifique la configuración apropiada del parámetro.
- En **Proveedor de valores**, en la lista desplegable **Nombre**, seleccione el tipo de proveedor de valores que desee usar.
  Las opciones disponibles dependen de la configuración del tipo de parámetro que definió en **Parámetro**.
- En **Configuración**, especifique la configuración apropiada del proveedor de valores.
  Si desea ver o editar otro parámetro de la lista, haga clic en los botones Subir y Bajar para mostrar los detalles del parámetro apropiado.
- Haga clic en **Aceptar**.

5 Haga clic en **Guardar cambios**.

Cómo crear o modificar una vista de gráfico para un informe personalizado

Cuando crea o modifica su propio informe personalizado de Notification Server, se puede definir una vista del informe. Una vista de informe es una manera determinada en la que se visualizan los resultados del informe. La configuración de un número de vistas distintas para un informe le permite personalizar los resultados del informe para diferentes usuarios. Una vista de gráfico le permite ver los resultados del informe en formato gráfico, como gráficos de barras, gráficos de líneas, gráficos circulares y gráficos de área.

Nota: Un conjunto de herramientas de terceros proporciona la funcionalidad que se usa en vistas de gráfico. Para obtener las descripciones completas de los componentes de diagramación, consulte la documentación que se proporciona en Dundas Data Visualization, Inc. (Dundas.com) .

Esta tarea es un paso en el proceso para crear y modificar los informes personalizados de Notification Server.

Ver "Creación y modificación de informes personalizados de Notification Server" en la página 452.

Para crear o modificar una vista de gráfico para un informe personalizado

1. En Symantec Management Console, en el menú **Informes**, haga clic en **Todos los informes**.
2. En el panel izquierdo, seleccione el informe que desee modificar.
3. En la página *Nombre del informe*, haga clic en **Editar**.
4. En la ficha **Vistas**, realice una de las siguientes acciones:
   - Para crear una nueva vista de gráfico, haga clic en **Agregar**.
   - Para modificar una vista de gráfico existente, en la lista desplegable **Ver**, seleccione la vista que desea modificar.
5. (Opcional) En el cuadro **Nombre**, escriba el nombre de la vista de gráfico.
6. En la lista desplegable **Tipo**, seleccione **Gráfico**.
7. En la lista desplegable **Tipo de gráfico**, seleccione el tipo de gráfico que desee usar.
8. En la lista desplegable **Estilo de gráfico**, seleccione el estilo que desee usar para representar el gráfico.

   Un estilo de gráfico es un conjunto predefinido de colores que se puede usar para representar el gráfico.
9. En los cuadros **Tamaño**, especifique la altura y el ancho del gráfico en píxeles.
10. En la lista desplegable **Etiquetas de gráfico**, seleccione la opción apropiada:

Todos	Muestra los valores de datos y los porcentajes reales.
Valores	Muestra los valores de datos reales, como el número de elementos de cada tipo.
Porcentaje	Muestra los datos como porcentajes, por ejemplo, el porcentaje de elementos de cada tipo.
Ninguno	No se muestran etiquetas.
Eje X solamente	Muestra los valores de datos para el eje X solamente. El eje Y no se etiqueta.

11 Para configurar la vista de gráfico, especifique las opciones apropiadas en las siguientes fichas:

Título	Permite especificar el texto del título del gráfico y la ubicación en la cual aparece.
Leyenda	Permite especificar el texto de la leyenda del gráfico y la ubicación en la cual aparece.
3D	Permite configurar el zoom 3D. El zoom 3D permite ampliar las áreas seleccionadas del gráfico según el tamaño completo de la ventana.
Eje X	Permite elegir la columna de resultados que se usará como eje X en el gráfico, especificar el texto del título y configurar el aspecto del eje X.
Eje Y	Permite elegir las columnas de resultados que se usarán como eje Y en el gráfico, especificar el texto del título y configurar el aspecto del eje Y.

Ver "Página Edición de informes personalizada: ficha Vistas para una vista de gráfico" en la página 539.

Para obtener más información, haga clic en la página y, después, presione **F1**.

12 Haga clic en **Guardar cambios**.

Cómo crear o modificar una vista de cuadrícula para un informe personalizado

Cuando crea o modifica su propio informe personalizado de Notification Server, puede crear y modificar las vistas de cuadrícula que desee en sus informes. Para cada vista de cuadrícula, se pueden seleccionar las columnas de resultados para incluir y especificar cómo se formatean los resultados.

Esta tarea es un paso en el proceso para crear y modificar los informes personalizados de Notification Server.

Ver "Creación y modificación de informes personalizados de Notification Server" en la página 452.

Para crear o modificar una vista de cuadrícula para un informe personalizado

1 En Symantec Management Console, en el menú **Informes**, haga clic en **Todos los informes**.

2 En el panel izquierdo, seleccione el informe que desee modificar.

3 En la página *Nombre del informe*, en la esquina superior derecha, haga clic en **Editar**.

4 En la ficha **Vistas**, realice una de las siguientes acciones:

Para crear una nueva vista de cuadrícula	Haga clic en **Agregar**.
Para modificar una vista de cuadrícula existente	En la lista desplegable **Ver**, seleccione la vista que desee modificar.

5 (Opcional) En el cuadro **Nombre**, escriba el nombre de la vista.

6 En la lista desplegable **Tipo**, seleccione **Cuadrícula**.

7 En la ficha **Columnas ocultas**, especifique las columnas de datos para incluir en la vista de cuadrícula del informe personalizado.

De forma predeterminada, la vista de cuadrícula incluye todas las columnas en los resultados de la consulta. Es posible ocultar cualquier columna de datos que no desee mostrar al usuario.

8 En la ficha **Formato avanzado** configure una plantilla de formato que aplique el etiquetado HTML a celdas o filas apropiadas en los resultados del informe.

Por ejemplo, en un informe de espacio libre en el disco del equipo, puede ser recomendable resaltar todos los equipos que tienen menos que la cantidad mínima especificada de espacio libre. Es posible crear una plantilla que aplique a las filas relevantes un fondo amarillo brillante y use texto en negrita en la celda Espacio libre.

Ver "Página Edición de informes personalizada: ficha Vistas para una vista de cuadrícula" en la página 542.

Para obtener más información, haga clic en la página y, después, presione **F1**.

9 (Opcional) Para obtener una vista previa de la cuadrícula con la configuración actual, haga clic en **Vista previa**.

10 Haga clic en **Guardar cambios**.

Cómo configurar acciones de examinación de niveles inferiores para un informe personalizado

Cuando crea o modifica su propio informe personalizado de Notification Server, se puede configurar un examen de niveles inferiores de informes. El examen de niveles inferiores de un informe es una acción que se realiza cuando el usuario hace clic en un elemento en los resultados del informe. Es posible configurar las

exploraciones de niveles inferiores para que un informe permita al usuario obtener información adicional a través de los resultados del informe. Al explorar los niveles inferiores de un elemento, se abre la vista correspondiente, que puede ser otro informe o una URL (por ejemplo, la Consola del administrador de recursos).

Es posible configurar varias exploraciones de niveles inferiores en un informe para realizar diferentes acciones en diferentes tipos de recursos.

Para cada examen de niveles inferiores, se puede especificar la vista en la cual el examen de niveles inferiores está disponible y cómo el usuario activa el examen de niveles inferiores. Es posible también especificar la acción que se realiza y los parámetros que se usan en la acción.

Es posible crear varios informes de examen de niveles inferiores, que son grupos de informes que se vinculan a una estructura jerárquica. Esta estructura puede permitir al usuario del informe seleccionar un elemento en un conjunto de resultados del informe y ejecutar otros informes. Los informes de examen de niveles inferiores pueden presentar información expandida para un conjunto más pequeño de recursos o pueden proporcionar información diferente en el recurso informando en diferentes campos.

Esta tarea es un paso en el proceso para crear y modificar los informes personalizados de Notification Server.

Ver "Creación y modificación de informes personalizados de Notification Server" en la página 452.

Para configurar las acciones de examinar de niveles inferiores de un informe personalizado

1. En Symantec Management Console, en el menú **Informes**, haga clic en **Todos los informes**.
2. En el panel izquierdo, seleccione el informe que desee modificar.
3. En la página *Nombre del informe*, haga clic en **Editar**.
4. En la ficha **Examinaciones de niveles inferiores**, realice una de las siguientes acciones:

Para agregar un nuevo examen de niveles inferiores	Haga clic en **Agregar**.
Para modificar un examen de niveles inferiores existente	En la lista desplegable **Examinar niveles inferiores**, seleccione el examen de niveles inferiores que desee modificar.

5. En el cuadro de diálogo **Nombre**, escriba un nombre apropiado para la exploración de niveles inferiores.

6 En **Conexión de acciones**, especifique la configuración siguiente:

Disponible en	Le permite especificar la vista apropiada del informe.
Evento	Le permite especificar el evento de usuario que es necesario para realizar la exploración de nivel inferior.
Realiza	Le permite especificar la acción que la exploración de nivel inferior realiza. Según la acción que se selecciona, cambian las opciones de **Configuración de acciones**.

7 En **Configuración de acciones**, especifique lo siguiente:

Exploración de nivel inferior que se debe informar	En la lista desplegable **Elemento de informe**, seleccione el informe cuya examinación de niveles inferiores desee ejecutar.
Mostrar menú contextual	No se aplica.
Abrir una dirección URL en una nueva ventana	En el cuadro **Abrir URL**, escriba la URL del elemento cuya acción de examinación de niveles inferiores desee abrir y, después, haga clic en **Establecer**.
Abrir una dirección URL en una nueva ventana para el NS remoto	En el cuadro **GUID del elemento de informe remoto**, escriba el GUID del informe remoto cuya acción de examinación de niveles inferiores desee abrir y después haga clic en **Establecer**.

8 En **Parámetros aprobados**, configure los parámetros que aprueban los valores de la acción de examinación de niveles inferiores.

Agregue o edite las siguientes opciones del parámetro:

Origen	El origen del valor del parámetro: ■ Parámetro denominado ■ Primer valor seleccionado ■ Fila seleccionada ■ Toda la selección
Información del campo	El nombre del campo de origen.
Parámetro de destino	El nombre del parámetro.

Tipo de parámetro de destino	El tipo de parámetro. La lista desplegable contiene todos los tipos de parámetro disponibles.

Es necesario que coincidan propiedades o valores del elemento seleccionado con los parámetros del examen de niveles inferiores. Este proceso asegura que se realice la acción apropiada. Por ejemplo, si desea que la acción de examinar de niveles inferiores abra el Administrador de recursos, puede aprobar el GUID de recurso apropiado como parámetro. Si desea que la acción de examinar de niveles inferiores ejecute un informe, puede aprobar los valores apropiados para la consulta de informe.

9 Haga clic en **Guardar cambios**.

Cómo especificar las propiedades avanzadas de un informe personalizado

Cuando crea o modifica su propio informe personalizado de Notification Server, puede restringir los resultados del informe al ámbito del usuario que ejecuta el informe. De forma predeterminada, al ejecutar un informe, se extrae de la CMDB el conjunto completo (sin alcance determinado) de resultados. El alcance de los resultados del informe se pueden determinar luego para garantizar que el usuario vea solamente los datos apropiados. Sin embargo, se puede determinar el alcance del informe para extraer solamente los datos apropiados de la CMDB.

Es posible también ejecutar el informe solamente como una instantánea. Para reducir al mínimo la carga en Notification Server, se recomienda ejecutar los informes grandes o usados frecuentemente como instantáneas. Cuando un usuario ejecuta el informe, los resultados se obtienen a partir de la última instantánea, en lugar de ejecutar la consulta del informe en la CMDB. Cuando se configura que un informe se ejecute solamente como instantánea, es posible especificar la antigüedad máxima de la instantánea. Cuando la instantánea llega a dicha antigüedad, la consulta del informe se ejecuta en la CMDB para extraer el resultado más reciente y actualizar la instantánea.

Esta tarea es un paso en el proceso para crear y modificar los informes personalizados de Notification Server.

Ver "Creación y modificación de informes personalizados de Notification Server" en la página 452.

Para especificar las propiedades avanzadas de un informe personalizado

1. En Symantec Management Console, en el menú **Informes**, haga clic en **Todos los informes**.
2. En el panel izquierdo, seleccione el informe que desee modificar.
3. En la página *Nombre del informe*, haga clic en **Editar**.
4. En la ficha **Opciones avanzadas**, realice una de las siguientes acciones:

Para promover la información de ámbito al origen de datos	Seleccione **Promover información sobre el ámbito al origen de datos**.
Para ejecutar el informe solamente como instantánea	1 Seleccione **Ejecutar informe siempre como una instantánea**. 2 En el cuadro **Actualizar automáticamente instantáneas con más de**, especifique la antigüedad en la cual se debe actualizar la instantánea con los resultados del informe más recientes.

5. Haga clic en **Guardar cambios**.

Capítulo 30

Visualización de información del recurso

En este capítulo se incluyen los temas siguientes:

- Acerca de los recursos
- Cómo ver información de clase de datos del recurso
- Cómo ver la información de tipo de asociación de recursos
- Cómo ver la información de tipo de recurso

Acerca de los recursos

Los recursos son los elementos con los cuales Notification Server funciona y almacena datos, por ejemplo, activos, facturas, órdenes de compra, proyectos, contratos y usuarios. Los datos sobre un recurso se agregan a la base de datos de administración de configuración (CMDB) usando una plantilla que se denomina tipo de recurso. Cada recurso de la CMDB tiene un tipo de recurso que especifique la información que se registra sobre el recurso. Por ejemplo, el nombre del recurso, la descripción, el modelo, el número de etiqueta de activo, el propietario, el departamento, etc.

Mientras más recursos se utilicen, se necesitará agrupar más recursos para propósitos de administración. Es posible usar vistas organizativas, grupos organizativos y filtros de recursos para ayudar a agrupar los recursos.

Ver "Cómo ver información de clase de datos del recurso" en la página 471.

Ver "Cómo ver la información de tipo de asociación de recursos" en la página 471.

Ver "Cómo ver la información de tipo de recurso" en la página 471.

Cómo ver información de clase de datos del recurso

Es posible ver información de clase de datos del recurso. Una clase de datos del recurso define uno o más campos y las propiedades de los campos que un recurso de esa clase puede tener.

Ver "Acerca de los recursos" en la página 470.

Para ver información de clase de datos del recurso

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Todas las configuraciones**.
2. En el panel izquierdo, expanda la carpeta **Configuración > Notification Server > Configuración de recursos y clases de datos > Clases de datos** y seleccione el tipo apropiado de clase de datos.

Cómo ver la información de tipo de asociación de recursos

Es posible ver la información del tipo de asociación de recursos. Una asociación de recursos es un vínculo entre dos recursos, tales como entre un usuario y un equipo. El usuario de un equipo tiene una asociación con ese equipo y viceversa.

Ver "Acerca de los recursos" en la página 470.

Para ver la información del tipo de de asociación de recursos

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Todas las configuraciones**.
2. En el panel izquierdo, expanda la carpeta **Configuración > Notification Server > Configuración de recursos y clases de datos > Asociaciones de recursos** y seleccione el tipo apropiado de asociación de recursos.

Cómo ver la información de tipo de recurso

Es posible ver la información de tipo de recurso, tales como el tipo de recursos básicos y las asociaciones de recursos que se aplican al tipo de recurso. Es posible también ver las clases de datos que se incluyen en el tipo de recurso.

Ver "Acerca de los recursos" en la página 470.

Para ver la información de tipo de recurso

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Todas las configuraciones**.
2. En el panel izquierdo, expanda la carpeta **Configuración > Notification Server > Configuración de recursos y clases de datos > Tipos de recursos** y seleccione el tipo apropiado de recurso.
3. En la página **Información sobre el tipo de recurso**, en la ficha **Configuración**, consulte la siguiente información sobre el tipo de recurso:

Detalles de tipo de recurso	Nombre y descripción del tipo de recurso y el tipo de recurso básico.
Tipos de asociación	Asociaciones de recursos que se aplican al tipo de recurso. De forma predeterminada, solamente se muestran los que se aplican directamente. Para mostrar asociaciones de recursos, compruebe **Mostrar los tipos de asociación heredados**.
Clases de datos	Clases de datos que se incluyen en el tipo de recurso. De forma predeterminada, se muestran todas las clases de datos. Para cambiar la vista: 1 Haga clic en alguna de las siguientes opciones: Editable: muestra las clases de datos que se pueden editar. Todos: muestra todas las clases de datos. Esta selección funciona en clases de datos disponibles. 2 (Opcional) Para ocultar clases de datos heredadas, anule la selección de **Mostrar clases de datos heredadas**.

Ningún cambio que se realizan se conserva cuando sale de la página **Información sobre el tipo de recursos**. La configuración predeterminada se restaura la próxima vez que se abre la página.

Sección 7

Cómo administrar datos de la CMDB con Data Connector

- Capítulo 31. Introducción a Data Connector
- Capítulo 32. Realizar tareas de administración de datos

Capítulo 31

Introducción a Data Connector

En este capítulo se incluyen los temas siguientes:

- Acerca de Data Connector
- Cómo funciona Data Connector
- Acciones que pueden llevarse a cabo con Data Connector

Acerca de Data Connector

Data Connector es un componente de Symantec Management Platform que permite transferir datos entre los orígenes de datos externos y la base de datos de administración de configuración (CMDB). La capacidad de transferir datos permite aprovechar los datos que ya existen en la CMDB u otras aplicaciones. Las transferencias de datos se pueden programar, de modo que las actualizaciones se pueden hacer regular y automáticamente para mantener los datos actualizados. Data Connector admite muchos formatos de datos: OLEDB, ODBC, LDAP, XML y CSV.

Data Connector además permite manipular los datos que ya están en la CMDB. Esta capacidad le permite normalizar y corregir fácilmente errores en sus datos. Por ejemplo, puede usar Data Connector para normalizar nombres de compañía para que los datos sean coherentes.

Ver "Cómo funciona Data Connector" en la página 475.

Cómo funciona Data Connector

Data Connector transfiere datos usando definiciones del origen de datos y reglas de transferencia de datos. Una definición de origen de datos define los parámetros para trabajar con un destinatario de datos o de origen de datos determinado (generalmente denominado origen de datos). Los parámetros pueden incluir la ubicación del origen de datos, el nombre, el tipo de transferencia de datos y las credenciales necesarias para acceder al origen de datos.

Data Connector admite los tipos de origen de datos CSV, LDAP, ODBC, OLEDB y XML.

Una regla de transferencia de datos configura los detalles de una transferencia de datos, tales como los siguientes:

- Una definición de origen de datos que se usa para la transferencia
- El tipo de recurso que se requiere en la transferencia
- Asignaciones entre los campos que se requieren en la transferencia
- Si la transferencia es una importación o una exportación

Diversos tipos de reglas de transferencia de datos están disponibles para distintos tipos de transferencias de datos:

Exportación de recursos masivos	Una manera eficiente de exportar recursos masivos de un informe o un recurso de destino a un archivo XML de evento de Notification Server (NSE). Puede también usar este tipo de regla para exportar historiales de cambio de recurso.
Importación de filtro	Especifica la pertenencia a los filtros de Symantec Management Platform importando la pertenencia de filtro de un origen de datos.
Importación de grupos organizativos	Especifica las pertenencias del grupo y de la vista organizativa de Symantec Management Platform importando la pertenencia del grupo o de la vista organizativa de un origen de datos.
Exportación de informes	Exporta los datos del informe a un origen de datos que tiene una definición de origen de datos que permite exportar.
Transferencia de datos de recursos	Transfiere (importa o exporta) los datos de recursos entre un origen de datos y la CMDB.

Para automatizar el proceso de transferencia de datos, se puede programar cada regla de transferencia de datos para ejecutarse en un momento específico. Las reglas de transferencia de datos se pueden además ejecutar con las tareas de

Symantec Management Platform. Después de las transferencias de datos, se pueden usar informes y archivos de registro predefinidos para analizar los resultados de las transferencias de datos.

Data Connector además permite manipular los datos que ya están en la CMDB con las reglas de CMDB. Estas reglas le permiten normalizar datos o resolver otros problemas de coherencia con los datos de la CMDB. Para manipular la CMDB, se necesita CMDB Solution.

Ver "Acerca de Data Connector" en la página 474.

Ver "Acciones que pueden llevarse a cabo con Data Connector" en la página 476.

Acciones que pueden llevarse a cabo con Data Connector

Data Connector le permite transferir datos entre la CMDB y un origen de datos y manipular datos dentro de la CMDB.

Es posible realizar las actividades de transferencia de los datos siguientes con Data Connector:

- Transferir (importar y exportar) los datos de recursos entre un origen de datos y la CMDB.
  Ver "Cómo importar y exportar datos" en la página 477.
- Importar la información de pertenencia al filtro, incluso agregar o quitar la pertenencia de recursos de uno o más filtros.
- Importar la vista organizativa y las pertenencias al grupo.
- Exportar un informe.
- Exportar datos de recursos en masa.

Data Connector además le permite manipular datos dentro de la CMDB. Por ejemplo, se puede normalizar o cambiar un conjunto de datos dentro de la CMDB. Para manipular los datos dentro de la CMDB, es necesario tener CMDB Solution.

Capítulo 32

Realizar tareas de administración de datos

En este capítulo se incluyen los temas siguientes:

- Cómo importar y exportar datos
- Cómo crear una clase de datos virtual
- Configurar las opciones de depuración del registro detallado de Data Connector

Cómo importar y exportar datos

Es necesario realizar varios pasos para transferir los datos entre la base de datos de administración de configuración (CMDB) y un origen de datos.

Tabla 32-1 Proceso para importar y exportar datos

Paso	Acción	Descripción
Paso 1	Cree un archivo de datos.	Primero, es necesario crear un archivo de datos y completarlo con los valores. Es posible incorporar los datos manualmente o con un proceso externo. Cuando se agregan nombres de columna como primera fila en el archivo de datos, la regla de importación de datos le permite hacer coincidir las columnas a las clases de datos de CMDB más fácilmente Es posible también preprocesar los datos en el origen de datos externo antes de importarlos en el CMDB. Ver "Acerca de preprocesar datos antes de importar los datos" en la página 479.

Paso	Acción	Descripción
Paso 2	Cree un origen de datos.	Se definen orígenes de datos usando definiciones de orígenes de datos. Las definiciones de orígenes de datos definen los parámetros que se deben especificar para trabajar con el origen de datos. Por ejemplo, una definición de orígenes de datos puede definir ubicaciones de bases de datos o de archivos, nombres de servidores y credenciales de acceso. Ver "Cómo crear una definición de origen de datos" en la página 479.
Paso 3	Cree una regla de la transferencia de datos.	La regla de la transferencia de datos le permite configurar la transferencia de datos. Las reglas de la transferencia de datos especifican los parámetros de la transferencia de datos, tales como la programación para la transferencia de datos, las asignaciones de la tabla de datos de entrada y salida y la dirección de la transferencia de datos. Ver "Crear una regla de transferencia de datos" en la página 480.
Paso 4	(Opcional) Cree una llave de búsqueda del recurso.	Una llave de búsqueda del recurso es un conjunto de columnas de la clase de datos que se usa para hacer coincidir los recursos entre el CMDB y el origen de datos. Ver "Crear una llave de búsqueda del recurso" en la página 481.
Paso 5	(Opcional) Ejecute una regla de transferencia de datos como tarea.	Es posible programar una tarea para que ejecute una regla de transferencia de datos. Ver "Cómo ejecutar una regla de transferencia de datos como tarea" en la página 482.
Paso 6	Compruebe los resultados de una transferencia de datos.	Es posible usar informes predefinidos para verificar que las transferencias de datos se realizaron correctamente. Ver "Cómo ver resúmenes de transferencia de datos" en la página 483.
Paso 7	(Opcional) Compruebe el estado de las reglas de transferencia de datos.	Es posible comprobar el estado de las reglas de transferencia de datos. La verificación de integridad asegura que no haya problemas causados por los cambios a la regla que puedan evitar que una transferencia de datos se complete correctamente. Ver "Comprobación del estado de las reglas de la transferencia de datos" en la página 483.

Paso	Acción	Descripción
Paso 8	(Opcional) Administre los datos importados.	Es posible crear reglas de CMDB que le permitan limpiar, normalizar o realizar cambios masivos a los datos en el CMDB. Ver "Crear una regla de CMDB para editar datos de CMDB" en la página 484. Ver "Cómo ejecutar una regla de CMDB como tarea" en la página 485.

Acerca de preprocesar datos antes de importar los datos

Al importar los datos de un origen de datos externo en la base de datos de administración de configuración (CMDB), se pueden manipular los datos antes de que se importen los datos. Este proceso previo de los datos le permite manipular los datos del origen de datos sin cambiar los datos en la ubicación original.

Se escribe una función de preproceso de los datos usando la programación de C#. La cantidad de preprocesos que se pueden hacer está limitada solamente por las acciones que pueden llevarse a cabo con la programación de C#. Una función de preproceso de los datos en C# toma una tabla de los datos como parámetro de la entrada. Es posible escribir el código de C# para manipular la tabla de los datos y su contenido. Una tabla actualizada de los datos entonces se devuelve como el valor devuelto del método. La tabla de los datos devueltos contiene los datos para el origen de datos durante la importación.

Para comprender mejor cómo el preproceso se puede usar, considere el ejemplo siguiente. Se hace un origen de datos OLEDB configurado para usar la “Tabla A” de la “Base de datos A”. Una función de preproceso agrega dinámicamente una columna a la tabla. Además rellena la nueva columna con los datos derivados de las otras columnas en la tabla.

Esta tarea es un paso opcional en el proceso para importar y exportar datos.

Ver "Cómo importar y exportar datos" en la página 477.

Cómo crear una definición de origen de datos

Un origen de datos es un origen o un destinatario de los datos de la base de datos de administración de configuración (CMDB). Por ejemplo, un archivo CSV o una base de datos de ODBC puede ser un origen de datos.

Es posible transferir datos entre los siguientes tipos de orígenes de datos y la CMDB:

- CSV

- LDAP
- ODBC
- OLEDB
- XML
- Personalizado(a)

Una definición del origen de datos especifica cómo acceder a un origen de datos determinado. La definición incluye el tipo de origen de datos, la ubicación, el nombre de la tabla y la información de la autenticación. Para cada origen de datos al cual o del cual se desee transferir datos, se necesita una definición del origen de datos. Para diversos tipos de orígenes de datos, hay diversos tipos de definición del origen de datos. Algunos tipos de definiciones del origen de datos permiten importar y exportar datos de la CMDB. Otros tipos permiten solamente exportar o importar.

Es necesario crear una definición de origen de datos para cada origen de datos entre los cuales desea transferir datos.

Esta tarea es un paso en el proceso para importar y exportar datos.

Ver "Cómo importar y exportar datos" en la página 477.

Para crear una definición de origen de datos

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Todas las configuraciones**.
2. En el panel izquierdo, expanda **Configuración > Notification Server > Data Connector**.
3. Haga clic con el botón derecho en **Orígenes de datos** y, luego, haga clic en **Nuevo > *Origen de datos***.
4. En el panel derecho, especifique los valores apropiados.

   Para obtener más información, haga clic en la página y, después, presione **F1**.
5. (Opcional) Haga clic en **Origen de datos de prueba** para probar el acceso al origen de datos.
6. Haga clic en **Guardar cambios**.

Crear una regla de transferencia de datos

Para que pueda transferir los datos entre la base de datos de administración de configuración (CMDB) y un origen de datos, es necesario especificar las opciones de transferencia de datos. Por ejemplo, es necesario especificar lo siguiente:

- El tipo de datos que se transfiere

- Si los datos están importados o exportados del origen de datos
- Cuáles de los datos se transfieren del origen de datos
- Cuándo ocurre la transferencia de datos

Para especificar las opciones de una transferencia de datos, se usa una regla de transferencia de datos. Varios tipos de reglas de transferencia de datos están disponibles. El que se usa depende del tipo de información que desea transferir.

Antes de usar una regla de transferencia de datos en un entorno de producción, recomendamos probar la regla. Use la opción **Regla de prueba** en la página aplicable de la regla de transferencia de datos.

Esta tarea es un paso en el proceso para importar y exportar datos.

Ver "Cómo importar y exportar datos" en la página 477.

Para crear una regla de transferencia de datos

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Todas las configuraciones**.
2. En el panel izquierdo, expanda **Configuración > Notification Server > Data Connector**.
3. Haga clic con el botón derecho en **Reglas de importación/exportación** y, luego, haga clic en **Nueva > *Regla de transferencia de datos***.
4. En el panel derecho, especifique las asignaciones de la columna y una programación para la regla.

   Para obtener más información, haga clic en la página y, después, presione **F1**.
5. Haga clic en **Guardar cambios**.

Crear una llave de búsqueda del recurso

Una llave de búsqueda de recursos es un valor único para un tipo de recurso que se usa para hacer coincidir los recursos entre la base de datos de administración de configuración (CMDB) y el origen de datos

Esta tarea es un paso en el proceso para importar y exportar datos.

Ver "Cómo importar y exportar datos" en la página 477.

Para crear una llave de búsqueda de recursos

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Todas las configuraciones**.
2. En el panel izquierdo, expanda **Configuración > Notification Server > Conector**.
3. Haga clic con el botón derecho en **Claves de búsqueda de recursos** y haga clic en **Nueva > Clave de búsqueda de recursos**.
4. En el panel derecho, especifique la configuración siguiente:

Tipo de recurso de destino	Tipo de recurso para el cual se especifica la llave de búsqueda.
Seleccionar una clase de datos	Le permite seleccionar la clase de datos que contiene el valor que desee usar como llave de búsqueda.
Utilizar en clave	Casillas de verificación para especificar la llave de búsqueda.

5. Haga clic en **Guardar cambios**.

Cómo ejecutar una regla de transferencia de datos como tarea

Es posible ejecutar una regla de transferencia de datos como tarea. Ejecutar una regla como tarea permite a la regla ejecutarse con varias tareas que se incluyan en un único trabajo.

Esta tarea es un paso en el proceso para importar y exportar datos.

Ver "Cómo importar y exportar datos" en la página 477.

Para ejecutar una regla de la transferencia de datos como tarea

1. En Symantec Management Console, en el menú **Administrar**, haga clic en **Tareas y trabajos**.
2. En el panel izquierdo, haga clic con el botón derecho en la carpeta donde desee agregar la tarea y haga clic en **Nuevo > Trabajo o tarea**.
3. En el panel izquierdo del cuadro de diálogo **Crear una nueva tarea**, haga clic en **Tareas del servidor > Ejecutar regla de conector**.
4. En el panel derecho, especifique un nombre para la tarea y seleccione una regla de transferencia de datos para que la tarea se ejecute.

5 Haga clic en **Aceptar**.

6 En el panel derecho, especifique una programación para la regla.

Ver "Configuración de una programación" en la página 123.

Ver "Ejecución de un trabajo o una tarea" en la página 421.

Para obtener más información, haga clic en la página y después presione **F1**.

Cómo ver resúmenes de transferencia de datos

Es posible ver los resultados de las transferencias de datos, que pueden incluir número de recursos, cantidades de filas, fechas y horas de transferencia, y origen de datos, a través de informes predefinidos. Estos informes pueden ser útiles para realizar el seguimiento de las transferencias de datos.

Esta tarea es un paso en el proceso para importar y exportar datos.

Ver "Cómo importar y exportar datos" en la página 477.

Para ver los resúmenes de transferencia de datos

1 En Symantec Management Console, en el menú **Informes**, haga clic en **Todos los informes**.

2 En el panel izquierdo, expanda **Informes > Administración de Notification Server > Conector** y después haga clic en el informe que desee ver.

Comprobación del estado de las reglas de la transferencia de datos

Es posible comprobar el estado (funcionamiento apropiado) de todas las reglas de la transferencia de datos mediante tareas predefinidas. Las tareas de verificación de integridad prueban cada regla. Son el equivalente de hacer clic en la opción **Regla de prueba** asociada con cada página de la regla para cada regla.

Realizar la verificación de integridad valida que las reglas y las definiciones del origen de datos estén configuradas correctamente. Cualquier error durante las pruebas se informa y se puede ver desde Estado de tarea de cada tarea de verificación de integridad ejecutada.

Las tareas predefinidas, como otras tareas, se pueden programar para ejecutarse de forma inmediata, en un momento específico o periódicamente.

Esta tarea es un paso en el proceso para importar y exportar datos.

Ver "Cómo importar y exportar datos" en la página 477.

Para comprobar el estado de las reglas de la transferencia de datos

1. En Symantec Management Console, en el menú **Administrar**, haga clic en **Tareas y trabajos**.
2. En el panel izquierdo, expanda **Trabajos y tareas de sistema > Notification Server > Conector** y después haga clic en **Tarea de verificación de integridad de las reglas del conector** o **Tarea de comprobación de integridad de la regla de la CMDB**.
3. En el panel derecho, especifique una programación para ejecutar la tarea.

   Ver "Adición de una programación a una política, una tarea o un trabajo" en la página 424.

   Ver "Configuración de una programación" en la página 123.

   Para obtener más información, haga clic en la página y después presione **F1**.
4. Una vez que la tarea se ejecute, vaya a la sección **Estado de tarea** para ver el estado de cada una de las reglas de la transferencia de datos.

Crear una regla de CMDB para editar datos de CMDB

Las reglas de CMDB son reglas personalizadas creadas por usted para administrar datos y tareas. Las reglas de CMDB le permiten manipular los datos que están ya en CMDB. Estas reglas le permiten normalizar datos o resolver otros problemas de coherencia con los datos de la CMDB.

Es posible crear sus propias reglas de CMDB, donde se dirija a un grupo de recursos basados en su tipo y sus propiedades y, después, es posible realizarles cambios. Para crear una regla, es necesario definir los criterios para los recursos de destino, los cambios que ocurrirán y el tipo de acción que se realizará. Es posible probar las reglas de CMDB personalizadas antes de ejecutarlas en un entorno de producción, crear programaciones y notificar al personal relevante. Las reglas de CMDB se pueden ejecutar, además, usando tareas y trabajos.

Tenga en cuenta que el uso de las reglas de CMDB requiere CMDB Solution.

Advertencia: Las reglas de CMDB son eficaces y pueden alterar cantidades extensas de datos. Antes de usar una regla de CMDB personalizada en un entorno de producción, Symantec recomienda encarecidamente probar la regla haciendo clic en la opción **Regla de prueba** en la página **Regla de CMDB**.

Esta tarea es un paso en el proceso para importar y exportar datos.

Ver "Cómo importar y exportar datos" en la página 477.

Para crear una regla de CMDB para editar datos de CMDB

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Todas las configuraciones**.
2. En el panel izquierdo, expanda **Configuración > Notification Server > Conector**.
3. Haga clic con el botón derecho en **Reglas de CMDB** y haga clic en **Nueva** > **Regla de CMDB**.
4. En el panel derecho, especifique los valores para la regla.

   Para obtener más información, haga clic en la página y después presione **F1**.
5. Haga clic en **Guardar cambios**.

Cómo ejecutar una regla de CMDB como tarea

Es posible ejecutar una regla de CMDB usando una tarea, que le permite ejecutar la regla junto con una serie de tareas en un trabajo.

Ver "Crear una regla de CMDB para editar datos de CMDB" en la página 484.

Nota: Las tareas definidas por el usuario de Connector Solution 6.5 no se migran automáticamente en el producto actual. Es necesario reconstruir manualmente estas tareas. Además, la capacidad para que una tarea permita ejecutar varias reglas en un orden especificado, se ha transferido a los trabajos. Cada tarea puede ejecutar solamente una única regla.

Esta tarea es un paso en el proceso para importar y exportar datos.

Ver "Cómo importar y exportar datos" en la página 477.

Para ejecutar una regla de CMDB como una tarea

1. En Symantec Management Console, en el menú **Administrar**, haga clic en **Tareas y trabajos**.
2. En el panel izquierdo, haga clic con el botón derecho en la carpeta donde desee agregar la tarea y haga clic en **Nuevo > Trabajo o tarea**.
3. En el panel izquierdo del cuadro de diálogo **Crear una nueva tarea**, haga clic en **Tareas del servidor > Ejecutar regla de CMDB**.
4. En el panel derecho, especifique un nombre para la tarea y seleccione una regla de CMDB para que la tarea se ejecute.

5 Haga clic en **Aceptar**.

6 En el panel derecho, especifique una programación para ejecutar la regla.

Ver "Adición de una programación a una política, una tarea o un trabajo" en la página 424.

Ver "Configuración de una programación" en la página 123.

Cómo crear una clase de datos virtual

Las clases de datos virtuales le permiten integrar datos de sistema de otro fabricante con la CMDB de Symantec Management Platform sin la necesidad de importar los datos en la CMDB.

Los datos externos que se asignan a una clase de datos virtuales aparecen como una clase de datos normal de recursos en la CMDB. Las clases de datos virtuales proporcionan una integración perfecta con las funciones de elaboración de informes de Symantec Management Platform. Es posible usar el generador de informes para crear los informes de recursos basados en clases de datos virtuales. El informe pregunta los datos directamente del origen de datos externo cuando se ejecuta el informe.

Los servidores vinculados a estos sistemas se deben configurar inicialmente en SQL Server antes de poder usar clases de datos virtuales. Consulte la documentación de Microsoft sobre los servidores vinculados (http://msdn.microsoft.com/en-us/library/ms188279(SQL.90).aspx) para obtener más información.

Es necesario tener el privilegio “Administrar conector de datos” para crear, editar o eliminar una clase de datos virtual. Para editar una clase de datos virtual, se debe además tener el permiso de escritura en la clase de datos virtuales.

Para crear una clase de datos virtual editable

1 En Symantec Management Console, en el menú **Configuración**, haga clic en **Todas las configuraciones**.

2 En el panel izquierdo, expanda **Configuración > Notification Server > Configuración de recursos y clases de datos**.

3 Haga clic con el botón derecho en **Clase de datos** y después haga clic en **Nueva > Clase de datos virtual**.

4 Haga clic en **Guardar cambios**.

Configurar las opciones de depuración del registro detallado de Data Connector

Es posible configurar la depuración de los archivos de registro de la regla. La depuración se realiza durante la programación diaria estándar.

Para configurar las opciones de depuración del registro detallado de Data Connector

1. En Symantec Management Console, en el menú **Configuración**, haga clic en **Todas las configuraciones**.
2. En el panel izquierdo, expanda **Configuración > Notification Server > Conector** y después haga clic en **Política de depuración del conector**.
3. En el panel derecho, especifique las opciones de depuración del archivo de registro de la regla.
4. Haga clic en **Guardar cambios**.

Apéndice A

Privilegios y permisos de seguridad

En este Apéndice se incluyen los temas siguientes:

- Categorías de privilegios de seguridad
- Categorías de permisos de seguridad
- Privilegios del perfil de conexión
- Privilegios de administración
- Privilegios del sistema
- Privilegios de credenciales
- Privilegios de directorio de flujo de trabajo
- Privilegios de Symantec Management Console
- Privilegios de Software Management
- Privilegios del menú contextual
- Menú contextual: Privilegios de muestras del conector
- Privilegios de jerarquía
- Privilegios de las acciones
- Establecer privilegios de estados de los activos
- Permisos de administración de recursos
- Permisos del sistema

- Permisos de Task Server
- Permisos de informes
- Permisos de políticas
- Permisos de carpeta
- Permisos de filtro
- Permisos del perfil de conexión
- Permisos de Credential Manager

Categorías de privilegios de seguridad

Un privilegio permite que un usuario realice una acción determinada en Symantec Management Platform o en elementos en Symantec Management Console. Para realizar una acción en un elemento, el rol de usuario debe tener el permiso necesario sobre el elemento. Los privilegios que puede asignar a un rol de seguridad se agrupan en categorías. Sin embargo, cuando se asignan privilegios a un rol de seguridad, es necesario seleccionar los privilegios apropiados individualmente.

Ver "Asignación de privilegios a un rol de seguridad" en la página 93.

Tabla A-1 Categorías de privilegios de seguridad

Categoría de privilegio	Descripción
Privilegios del perfil de conexión	Le permite crear y modificar perfiles de conexión. Ver "Privilegios del perfil de conexión" en la página 492.
Privilegios de administración	Le permite crear elementos de administración, como filtros, destinos, informes y tareas en Symantec Management Platform. Ver "Privilegios de administración" en la página 492.
Privilegios del sistema	Le permite realizar actividades de administración, como configurar la seguridad, administrar la jerarquía e importar archivos XML en Symantec Management Platform. Ver "Privilegios del sistema" en la página 494.
Privilegios de credenciales	Le permite usar Credential Manager para crear y modificar las credenciales. Estas credenciales no son las mismas que las credenciales internas y las credenciales de Windows que se asocian a las cuentas de usuario. **Nota:** Credential Manager es un componente de Symantec Management Platform extendido, de forma que no se puede instalar en su entorno. Ver "Privilegios de credenciales" en la página 496.

Categoría de privilegio	Descripción
Privilegios de directorio de flujo de trabajo	Le permite publicar flujos de trabajo de Workflow Designer en Notification Server como acción de la tarea o del elemento (una opción en el menú contextual). Ver "Privilegios de directorio de flujo de trabajo" en la página 497.
Privilegios de la consola	Le permite personalizar Symantec Management Console. Estos privilegios incluyen la posibilidad de editar el menú y crear páginas del portal, elementos web y vistas. Ver "Privilegios de Symantec Management Console" en la página 497.
Privilegios de Software Management	Le permite conceder capacidades específicas al rol de usuario y permitir que el usuario realice tareas específicas en la vista **Software** y en la ventana **Catálogo de software.** Estos privilegios también brindan la capacidad de crear la Biblioteca de software y de generar e importar recursos de software. Ver "Privilegios de Software Management" en la página 498.
Privilegios del menú contextual	Le permite realizar acciones generales en los elementos que están en Symantec Management Console. Cuando haga clic con el botón derecho en un elemento, las opciones relevantes para este elemento estarán disponibles en el menú contextual. Estos privilegios incluyen la posibilidad de eliminar un elemento, editar vistas, vínculos web y vínculos de elementos, e iniciar, detener y programar tareas. Ver "Privilegios del menú contextual" en la página 500.
Privilegios de muestras del conector	Ejemplos de acciones contextuales creadas por el usuario. Ver "Menú contextual: Privilegios de muestras del conector" en la página 502.
Privilegios de jerarquía	Le permite administrar una réplica de la jerarquía. Estos privilegios le permiten incluir o excluir elementos específicos de la réplica de la jerarquía y, a la vez, replicar estos elementos inmediatamente. Ver "Privilegios de jerarquía" en la página 502.
Privilegios de las acciones	Le permite realizar acciones relevantes para Software Management Framework. Las soluciones adicionales que están instaladas en Symantec Management Platform pueden agregar otros privilegios a esta categoría. Ver "Privilegios de jerarquía" en la página 502.
Establecer privilegios de estados de los activos	Le permite cambiar el estado de un activo. Estos privilegios le permiten configurar el estado de un recurso en Activo o Retirado. Las soluciones que están instaladas en Symantec Management Platform pueden agregar más privilegios. Ver "Establecer privilegios de estados de los activos" en la página 505.

Categorías de permisos de seguridad

Los permisos en un elemento en Symantec Management Console determinan el acceso que tiene un rol de seguridad a ese elemento. Los permisos en elementos se aplican a los roles de seguridad, no a las cuentas de usuario individuales. Por ejemplo, el permiso de lectura en un elemento permite al usuario ver el elemento, y el permiso de escritura en el elemento permite al usuario modificarlo.

Ver "Asignación de permisos de seguridad a carpetas y elementos" en la página 103.

Los permisos se usan con privilegios para determinar qué acciones puede realizar un rol de seguridad en un elemento. Por ejemplo, para eliminar un elemento, un rol de seguridad debe tener el privilegio de eliminación y el permiso para eliminar ese elemento en particular. Solamente tener el privilegio de eliminación o el permiso para eliminar ese elemento no es suficiente.

Es posible especificar los permisos que se aplican a cada carpeta o elemento para cada rol de seguridad. Los permisos que se aplican directamente a una carpeta o un elemento (permisos no heredados) se combinan con los permisos que se heredan de la carpeta principal. Los permisos combinados determinan el acceso que tiene el rol de seguridad a esa carpeta o ese elemento en particular.

De forma predeterminada, las carpetas y los elementos secundarios heredan todos los permisos en una carpeta. Es posible modificar la herencia de permisos para adaptarse a sus requisitos.

Las categorías de permisos de seguridad enumeran y describen las categorías de los permisos de seguridad que puede configurar para cada rol.

Tabla A-2 Categorías de permiso de seguridad

Categoría de permiso	Descripción
Administración de recursos	Estos permisos se aplican a recursos. Ver "Permisos de administración de recursos" en la página 505.
Sistema	Estos permisos se aplican al sistema, como la lectura, la escritura y la eliminación de elementos. Ver "Permisos del sistema" en la página 506.
Task Server	Estos permisos se aplican a Task Server. Ver "Permisos de Task Server" en la página 506.
Informe	Estos permisos se aplican a los informes. Ver "Permisos de informes" en la página 507.

Categoría de permiso	Descripción
Política	Estos permisos se aplican a las políticas. Ver "Permisos de políticas" en la página 507.
Carpeta	Estos permisos se aplican a las carpetas. Ver "Permisos de carpeta" en la página 507.
Filtro	Estos permisos se aplican a los filtros. Ver "Permisos de filtro" en la página 508.
Perfil de conexión	Estos permisos le permiten usar perfiles de conexión. Ver "Permisos del perfil de conexión" en la página 508.
Credential Manager	Estos permisos le permiten usar Credential Manager. Ver "Permisos de Credential Manager" en la página 509.

Privilegios del perfil de conexión

Los privilegios del perfil de conexión le permiten crear y modificar perfiles de conexión. Los perfiles de conexión almacenan la información necesaria para comunicarse con los equipos y otros dispositivos de red mediante los protocolos de red estándar de supervisión. Estos protocolos incluyen SNMP, WMI, WSMan y otros.

Ver "Categorías de privilegios de seguridad" en la página 489.

Ver "Asignación de privilegios a un rol de seguridad" en la página 93.

Tabla A-3 Privilegios del perfil de conexión

Privilegio	Descripción
Crear perfil de conexión	Le permite crear y modificar perfiles de conexión.

Privilegios de administración

Los privilegios de administración permiten crear elementos de administración, como filtros, destinos, informes y tareas, en Symantec Management Platform.

Ver "Categorías de privilegios de seguridad" en la página 489.

Ver "Asignación de privilegios a un rol de seguridad" en la página 93.

Tabla A-4 Privilegios de administración

Privilegio	Descripción
Crear configuración de agente	Permite crear una nueva directiva de configuración del agente de destino o clonar una directiva existente. La configuración del agente de destino es el parámetro general que controla a Symantec Management Agent, incluido cómo el agente se comunica con Notification Server. Ver "Configuración de las opciones de configuración del agente de destino" en la página 278.
Crear directivas de automatización	Permite crear nuevas directivas de automatización. Una política de automatización es dinámica y especifica acciones automatizadas para realizar en el equipo con Notification Server. Se dirige a los equipos apropiados cuando la directiva se activa y realiza cualquier acción requerida basada en el estado actual del equipo destino. Ver "Acerca de las políticas de automatización" en la página 391.
Crear filtros	Permite crear nuevos filtros de recursos. Un filtro de recurso, generalmente conocido como filtro, es una definición dinámica de un conjunto de recursos. Los filtros se utilizan con grupos organizativos para identificar los recursos (un destino de recursos) a los cuales se aplican una tarea o directiva. Ver "Acerca de los filtros de recursos" en la página 353.
Crear trabajos o tareas	Permite crear un nuevo trabajo o tarea o clonar un trabajo o tarea existente. Los trabajos pueden contener varias tareas y condiciones, lo que brinda gran flexibilidad al configurar la secuencia de trabajos que necesita. Ver "Cómo crear una tarea" en la página 418. Ver "Cómo crear un trabajo" en la página 418.
Crear ventanas de mantenimiento	Permite crear una nueva directiva de ventana de mantenimiento o clonar una directiva existente. Una ventana de mantenimiento se refiere a una hora y duración programada en cuanto se realicen operaciones de mantenimiento en un equipo administrado. Una directiva de ventana de mantenimiento define una o más ventanas de mantenimiento.
Crear nuevo trabajo de cliente	Le permite crear un trabajo de cliente. Los trabajos de cliente se implementan en equipos administrados mediante Task Server. El equipo administrado ejecuta el trabajo y envía informes a Notification Server. Ver "Cómo crear un trabajo" en la página 418.
Crear nuevo trabajo de servidor	Le permite crear un trabajo de servidor. Los trabajos de servidor se ejecutan en Notification Server. Ver "Cómo crear un trabajo" en la página 418.

Privilegio	Descripción
Crear grupos organizativos	Permite crear nuevas vistas y grupos organizativos. Una vista organizativa es un grupo jerárquico de recursos (como grupos organizativos) que refleja una estructura real, o vista, de su organización.
Crear informes	Permite crear un informe nuevo o clonar un informe existente. Ver "Creación y modificación de informes personalizados de Notification Server" en la página 452.
Crear destinos para recursos	Permite crear nuevos destinos de recursos. El destino de recursos, normalmente conocido como destino, es un marco de trabajo que permite aplicar tareas y directivas a una colección dinámica de recursos. El destino consiste en al menos una vista o un grupo organizativo y una cantidad de filtros. Los filtros reducen los recursos disponibles a fin de identificar los que desee. Ver "Acerca de los destinos de recursos" en la página 366.
Administración de tareas de Discovery	Le permite realizar tareas de detección de redes.

Privilegios del sistema

Los privilegios del sistema le permiten realizar actividades de administración, como configurar la seguridad, administrar la jerarquía e importar archivos XML en Symantec Management Platform.

Ver "Categorías de privilegios de seguridad" en la página 489.

Ver "Asignación de privilegios a un rol de seguridad" en la página 93.

Tabla A-5 Privilegios del sistema

Privilegio	Descripción
Cambiar seguridad	Le permite cambiar la configuración de seguridad en Symantec Management Platform. Puede crear roles de seguridad, asignar privilegios y cuentas de usuarios a roles de seguridad, así como también asignar permisos a elementos de administración para cada rol. Ver "Configuración de la seguridad de Symantec Management Platform" en la página 85.

Privilegio	Descripción
Crear reglas de CMDB	Le permite crear reglas de CMDB en Data Connector. Data Connector se usa para transferir datos entre el CMDB y un origen de datos, y manipular datos dentro de CMDB. Data Connector es parte de Symantec Management Platform extendida. Ver "Acerca de Data Connector" en la página 474.
Editar SQL directamente	Le permite crear o modificar consultas SQL en informes y filtros. Este privilegio además le permite editar la consulta de origen de datos y ver los resultados de la consulta del origen de datos de una **Consulta SQL sin procesar** para una política de automatización. Si el usuario es competente en SQL y conoce CMDB, este privilegio permite escribir informes muy eficientes y específicos. Sin embargo, también se le puede usar para evitar comprobaciones de seguridad. Por ejemplo, un usuario puede escribir una consulta que acceda a los recursos que están fuera de su ámbito. Es decir, los recursos no están en los grupos organizativos que el usuario tiene permiso para ver. **Advertencia:** Las consultas SQL que no están bien escritas pueden devolver resultados incorrectos o pueden ser ineficientes debido a que consumen demasiada memoria y tiempo de la CPU en el equipo CMDB. Además, una consulta SQL maliciosa puede eliminar, modificar o agregar datos en cualquier lugar en CMDB. Por lo tanto, este privilegio es muy sensible a la seguridad y solamente se otorga de forma predeterminada al rol de administradores de Symantec. Si permite que miembros de rol de seguridad editen SQL directamente, debe usar las credenciales de aplicación específica de informes para forzar a los informes a utilizar una cuenta con acceso restringido a CMDB Ver "Cómo definir una consulta SQL para un informe personalizado" en la página 459.
Importar/Exportar XML	Le permite importar elementos y recursos de archivos especialmente estructurados de XML y exportar elementos y recursos a los archivos de XML. Tenga cuidado cuando se cree un elemento o un recurso en Symantec Management Platform importando la información que se almacena en un archivo XML. Al crear un elemento de esta manera, se sobrepasan todas las comprobaciones de seguridad. Por ejemplo, un usuario puede crear un informe importando su XML incluso cuando no tiene los privilegios ni los permisos necesarios. En este ejemplo, el usuario necesita el privilegio Crear informes y el permiso Crear secundario de la carpeta en la cual se almacena el informe. Este privilegio es muy sensible a la seguridad. De forma predeterminada, solamente se otorga al rol de administradores de Symantec y no debe ser otorgado a aquellos que no lo son. Ver "Cómo guardar elementos de la consola como archivos XML" en la página 63.

Privilegio	Descripción
Administrar Data Connector	Le permite administrar Data Connector. Data Connector es parte de Symantec Management Platform extendida. Data Connector se usa para transferir datos entre el CMDB y un origen de datos, y manipular datos dentro de CMDB. Ver "Acerca de Data Connector" en la página 474.
Administrar la réplica de la jerarquía	Le permite crear y ejecutar reglas de réplica de la jerarquía. Las reglas de réplica de la jerarquía especifican lo que se está replicando en el Notification Server principal y en cualquier Notification Server secundario. Este privilegio además le permite acceder a las reglas de replicación independientes. Ver "Configurar la réplica de la jerarquía y las reglas de la réplica de la jerarquía" en la página 163.
Administrar jerarquía	Le permite agregar su Notification Server a una jerarquía o eliminarlo de una jerarquía. Es posible agregar su Notification Server a una jerarquía como servidor secundario de un Notification Server remoto existente o como su servidor principal. Recuerde que su Notification Server es en el que inicia sesión, que puede ser un inicio de sesión remoto. Precisa de este privilegio en ambos servidores de Notification Server para crear o cambiar una relación jerárquica entre ellos.
Asumir posesión	Le permite tomar posesión de una entidad de seguridad. Este privilegio otorgará al nuevo propietario permisos completos sobre la entidad. Por ejemplo, necesitará tomar posesión si todos los permisos sobre la entidad se eliminan de manera accidental. Ver "Propiedad de una carpeta o elemento" en la página 115.
Ver seguridad	Le permite ver la configuración de seguridad en Symantec Management Platform. Esta información incluye detalles de los roles de seguridad y las cuentas de usuario, los privilegios y los permisos que se asignan a cada rol.

Privilegios de credenciales

Los privilegios de credenciales le permiten crear nuevas credenciales en Credential Manager. Credential Manager proporciona una ubicación segura de almacenamiento para los nombres de usuario y las contraseñas. Las soluciones que están instaladas en Symantec Management Platform definen los tipos de credenciales que Credential Manager almacena.

Ver "Categorías de privilegios de seguridad" en la página 489.

Ver "Asignación de privilegios a un rol de seguridad" en la página 93.

Cuando se crea una credencial, solamente se concede acceso al creador. Si otros usuarios necesitan realizar una operación de administración que necesite una credencial, es necesario asignar este privilegio a la cuenta de usuario o al rol apropiado que contiene la cuenta de usuario.

Tabla A-6 Privilegios de credenciales

Privilegio	Descripción
Crear credencial	Le permite crear y modificar las credenciales en Credential Manager.

Privilegios de directorio de flujo de trabajo

Los privilegios de directorio de flujo de trabajo permiten publicar flujos de trabajo del diseñador del flujo de trabajo en Notification Server como acción de la tarea o del elemento (una opción en el menú contextual).

Workflow Designer es parte de la solución Workflow. Cuando se instala la solución Workflow, agrega una página a Symantec Management Console que le permite descargar e instalar Workflow Designer. No se incluye en Symantec Management Platform de forma predeterminada.

Ver "Categorías de privilegios de seguridad" en la página 489.

Ver "Asignación de privilegios a un rol de seguridad" en la página 93.

Tabla A-7 Privilegios de directorio de flujo de trabajo

Privilegio	Descripción
Registrar/eliminar registro de flujos de trabajo	Le permite publicar flujos de trabajo de Workflow Designer en Notification Server como acción de la tarea o del elemento (una opción en el menú contextual). Para más información, consulte la documentación de la solución Workflow.

Privilegios de Symantec Management Console

Los privilegios de Symantec Management Console le permiten personalizar Symantec Management Console. Estos privilegios incluyen la posibilidad de editar el menú y crear páginas del portal, elementos web y vistas.

Ver "Categorías de privilegios de seguridad" en la página 489.

Ver "Asignación de privilegios a un rol de seguridad" en la página 93.

Tabla A-8 Privilegios de Symantec Management Console

Privilegio	Descripción
Crear páginas del portal	Le permite crear nuevas páginas del portal. Una página del portal es una página de Symantec Management Console que se puede personalizar para satisfacer sus requisitos. El usuario tiene la posibilidad de usar una página del portal para consolidar la información clave en una sola página fácil de visualizar. Una página del portal permite mostrar el estado de Symantec Management Platform y de los equipos administrados, o cualquier otro tipo de información que se desee poner a disposición. Por ejemplo, se pueden incluir páginas web externas, páginas de intranet, fuentes RSS o aplicaciones propias. Necesita tener el permiso Crear secundario en la carpeta en la cual desea crear la nueva página del portal.
Crear elementos web	Le permite crear elementos web nuevos. Los elementos web son las minipáginas web que se pueden usar como componentes para páginas del portal. Un elemento web puede mostrar un informe o el contenido de una página web. Necesita tener el permiso Crear secundario en la carpeta en la cual desea crear el elemento web nuevo. Ver "Creación y modificación de elementos web" en la página 61.
Crear vistas	Le permite crear vistas nuevas. Una vista es un diseño de dos paneles con un árbol de navegación en el panel izquierdo y el contenido en el panel derecho. El árbol de navegación contiene vínculos a los elementos de Symantec Management Console y permite agrupar los elementos de diferentes partes de la consola en una estructura adecuada. Un elemento puede aparecer varias veces en una vista y en cualquier cantidad de vistas. Una vista puede incluir carpetas, vínculos de elementos y vínculos web. Ver "Acerca de las vistas de la consola" en la página 36.
Editar el menú de la consola	Le permite personalizar los menús de Symantec Management Console. Las opciones del menú que se proporcionan con Symantec Management Platform son de solo lectura y no se pueden modificar. Es posible agregar nuevos submenús y modificarlos según sea necesario. Los elementos del menú se pueden mover o eliminar, excepto los señalados como de solo lectura. Ver "Personalización del menú de la consola" en la página 53.

Privilegios de Software Management

Cada privilegio de **Software Management** concede capacidades específicas al rol de usuario y permite que el usuario realice tareas específicas en la vista **Software** y la ventana **Catálogo de software** de las vistas de consola mejoradas. Estos privilegios también brindan la capacidad de crear la Biblioteca de software y de

generar e importar recursos de software. Estos privilegios de **Software Management** no son de forma predeterminada parte de ningún rol de usuario. Es necesario asignar el privilegio relevante a un rol de usuario.

Ver "Categorías de privilegios de seguridad" en la página 489.

Ver "Asignación de privilegios a un rol de seguridad" en la página 93.

Tabla A-9 Privilegios de **Software Management**

Privilegio	Descripción
Crear productos de software y **Definir filtros de inventario de productos de software**	Este privilegio permite que el usuario use la búsqueda guardada del **Software recientemente detectado** en la vista **Software** para encontrar el software recién detectado. Este privilegio permite que el usuario use los paneles **Software recientemente detectado/definido** y **Software no administrado** en **Catálogo de software** para administrar el software. Para tener estas capacidades, es necesario asignar al rol de usuario los privilegios **Crear productos de software** y **Definir productos de software**.
Crear productos de software	Este privilegio permite que el usuario use el botón **Agregar producto** para abrir el cuadro de diálogo **Producto de software**. Este privilegio permite que el usuario introduzca datos en las áreas **Nombre**, **Compañía**, **Versión** y **Categoría** del cuadro de diálogo **Producto de software** para crear los productos de software. Si no asigna este privilegio al rol de usuario, el usuario no puede especificar la información en las áreas **Nombre**, **Compañía**, **Versión** y **Categoría** del cuadro de diálogo **Producto de software**.
Definir filtros de inventario de productos de software	Este privilegio permite que el usuario use la ficha **Identificar inventario** para definir los filtros del inventario del producto de software.
Configurar seguimiento de uso de software	Este privilegio permite que el usuario use el hipervínculo **Agregar archivos de programa** y la ficha **Medir/realizar seguimiento del uso** para configurar el seguimiento del uso del software.
Crear licencias de software	Este privilegio permite que el usuario use el botón **Administrar licencias** para crear las licencias de software.

Privilegio	Descripción
Administrar recursos de software	Le permite crear, importar, editar y eliminar los recursos de software. Un recurso de software está formado por los metadatos que describen una instancia específica de un producto de software. Un recurso de software proporciona una manera común para describir el software a fin de que todas las acciones relacionadas con el software puedan identificarlo con precisión. Normalmente, es necesario asignar privilegios de recursos de software a las cuentas de usuarios que entregan y administran software. Los roles de seguridad **Bibliotecario de software de Symantec** y **Administrador de activos** tienen este privilegio de forma predeterminada.
Administrar configuración de la biblioteca de software	Le permite crear y editar la **Configuración de la biblioteca de software**. La Biblioteca de software es la ubicación física del directorio de los archivos de paquete que se asocian al software en el Catálogo de software. Como la Biblioteca de software es un repositorio de las versiones definitivas y autorizadas de los paquetes, es necesario restringir el acceso a la biblioteca para mantener su integridad. Los roles de seguridad **Bibliotecario de software de Symantec** y **Administrador de activos** tienen este privilegio de forma predeterminada.
Crear entregas de software	Le permite crear las entregas de software (las tareas de **Entrega rápida** o de **Entrega de paquete** y la política de **Administrar entrega de software**) para el recurso de software seleccionado de la lista disponible del software. Le permite usar la función de arrastrar y colocar para iniciar la entrega de software de cualquier lista de software. Este privilegio además permite que el usuario use la ficha **Entrega** para crear las entregas de software.

Privilegios del menú contextual

Los privilegios del menú contextual (a veces denominados privilegios de acción de elemento) permiten realizar acciones generales sobre elementos en Symantec Management Console. Cuando haga clic con el botón derecho en un elemento, las opciones relevantes a este elemento estarán disponibles en el menú contextual. Estos privilegios incluyen la posibilidad de eliminar un elemento, editar vistas, vínculos web y vínculos de elementos, e iniciar, detener y programar tareas.

Ver "Categorías de privilegios de seguridad" en la página 489.

Ver "Asignación de privilegios a un rol de seguridad" en la página 93.

Tabla A-10 Privilegios del menú contextual

Privilegio	Descripción	Tipos de elementos a los que se aplica	Requisitos adicionales
Agregar grupo organizativo	Permite agregar un recurso a un grupo organizativo. Ver "Crear y configurar un grupo organizativo" en la página 344.	Todos los recursos	Permiso de escritura en el grupo organizativo.
Clonar	Le permite clonar un elemento.	Todos los tipos de elementos	Permiso de clon en el elemento.
Eliminar	Permite eliminar un elemento.	Todos los tipos de elementos	Permiso de eliminación en el elemento.
Editar el vínculo del elemento	Permite modificar un vínculo de elemento. Ver "Acerca de las vistas de la consola" en la página 36.	Solo vínculos de elementos.	Permiso de escritura en vínculo de elemento.
Editar regla	Permite editar una regla de inventario.	Sólo reglas de inventario.	Permiso de escritura en regla de inventario.
Editar vista	Permite editar una vista. Ver "Creación y modificación de vistas" en la página 57.	Sólo vistas.	Permiso de escritura en la vista.
Editar vínculo Web	Permite modificar un vínculo web. Ver "Acerca de las vistas de la consola" en la página 36.	Sólo vínculos web.	Permiso de escritura en vínculo web.
Programación	Permite programar una directiva. Ver "Cómo especificar una programación de política" en la página 387.	Sólo directivas.	Permiso de escritura en la directiva.
Programar tarea	Permite programar una tarea. Puede programar la tarea para que la misma se ejecute en una hora en particular o se repita en intervalos regulares. Ver "Adición de una programación a una política, una tarea o un trabajo" en la página 424.	Solo tareas.	Ejecutar permiso de tarea en la tarea.
Administrador de roles de seguridad	Le permite abrir el Administrador de roles de seguridad.	Todos los tipos de elementos	Permiso de escritura en el elemento.

Privilegio	Descripción	Tipos de elementos a los que se aplica	Requisitos adicionales
Iniciar tarea	Permite iniciar una tarea de manera inmediata. Ver "Ejecución de un trabajo o una tarea" en la página 421.	Solo tareas.	Ejecutar permiso de tarea en la tarea.
Detener tarea	Permite detener una tarea de manera inmediata.	Solo tareas.	Ejecutar permiso de tarea en la tarea.

Menú contextual: Privilegios de muestras del conector

Los privilegios de muestras del conector son ejemplos de acciones que el usuario puede crear haciendo clic con el botón derecho.

Ver "Categorías de privilegios de seguridad" en la página 489.

Ver "Asignación de privilegios a un rol de seguridad" en la página 93.

Tabla A-11 Menú contextual: Privilegios de muestras del conector

Privilegio	Descripción	Tipos de elementos a los que se aplica	Requisitos adicionales
Efectuar ping en el equipo	Permite efectuar un ping TCP/IP en un equipo.	Solamente recursos de equipos	Permiso de lectura en el grupo organizativo que contiene el equipo.

Privilegios de jerarquía

Los privilegios de jerarquía le permiten administrar una réplica de la jerarquía. Estos privilegios le permiten incluir o excluir elementos específicos de la réplica de la jerarquía y, a la vez, replicar estos elementos inmediatamente.

Ver "Categorías de privilegios de seguridad" en la página 489.

Ver "Asignación de privilegios a un rol de seguridad" en la página 93.

Tabla A-12 Privilegios de jerarquía

Privilegio	Descripción	Tipos de elementos a los que se aplica	Requisitos adicionales
Deshabilitar replicación	Le permite impedir a un elemento participar en la réplica de la jerarquía. Todos los elementos de administración y configuración, los roles de seguridad y los privilegios se replican de forma predeterminada. Esta opción está disponible solo cuando se utilizan reglas de réplica de la jerarquía personalizadas. Ver "Cómo configurar una réplica de la jerarquía personalizada" en la página 165.	Todos los tipos de elementos	Administrar privilegio de réplica de la jerarquía, permiso de escritura en el elemento.
Replicar ahora	Le permite replicar los datos seleccionados directamente desde Notification Server a todos los servidores de Notification Server secundarios sin incluirlos en la regla de replicación. Esta operación es una réplica que se realiza solamente una vez y de manera inmediata. Ver "Cómo replicar datos seleccionados manualmente" en la página 168.	Todos los tipos de elementos	Administrar privilegio de réplica de la jerarquía, permiso de escritura en el elemento.
Habilitar replicación	Permite la participación de un elemento en la réplica de la jerarquía. Todos los elementos de administración y configuración, los roles de seguridad y los privilegios se replican de forma predeterminada. Esta opción está disponible solo cuando se utilizan reglas de réplica de la jerarquía personalizadas. Ver "Cómo configurar una réplica de la jerarquía personalizada" en la página 165.	Todos los tipos de elementos	Administrar privilegio de réplica de la jerarquía, permiso de escritura en el elemento.

Privilegios de las acciones

Los privilegios de las acciones permiten realizar las acciones que son relevantes para Software Management Framework. Las soluciones adicionales que están instaladas en la Plataforma de administración Symantec pueden agregar otros privilegios a esta categoría.

Ver "Categorías de privilegios de seguridad" en la página 489.

Ver "Asignación de privilegios a un rol de seguridad" en la página 93.

Tabla A-13 Menú contextual: privilegios de acciones

Privilegio	Descripción	Tipos de elementos a los que se aplica	Requisitos adicionales
Asignar tipo	Asigna un tipo a un recurso de software no asignado en el Catálogo de software. Un recurso de software no asignado es un recurso que no se categoriza como una versión de software, una actualización ni un Service Pack.	Recursos de software solamente	
Crear el filtro de programas de software instalados	Crea filtros para encontrar equipos administrados por el software que está instalado en ellos.	Recursos de software solamente	
Exportación detallada	Exporta un recurso de software y cualquier información asociada del recurso a un archivo XML detallado.	Recursos de software solamente	
Editar la Línea de comandos	Abre la línea de comandos seleccionada para la edición en la página de edición del recurso de software.	Recursos de software solamente	
Editar el paquete	Abre el paquete seleccionado para la edición en la página de edición del recurso de software.	Recursos de software solamente	
Editar recursos de software	Abre el recurso de software seleccionado para la edición.	Recursos de software solamente	
Importar paquete	Cambia el origen de un paquete a la Biblioteca de software desde un origen diferente, como un directorio en el servidor o una ruta UNC.	Recursos de software solamente	
Fusionar recursos de empresa	Fusiona el recurso seleccionado de la compañía con otro recurso de la compañía. Este privilegio es útil si tiene dos entradas para la misma compañía, que tal vez se escribieron de forma levemente diferente, por ejemplo, “Symantec” y “Symantec Corporation”. Es posible seleccionar los elementos para combinar y especificar el nombre apropiado que se debe usar.		

Privilegio	Descripción	Tipos de elementos a los que se aplica	Requisitos adicionales
Resolver los recursos de software duplicados	Cuando dos recursos de software representan el mismo software, pero tienen diferentes identificadores, este cuadro de diálogo permite al usuario asociar ambos identificadores con un recurso de software.	Recursos de software solamente	

Establecer privilegios de estados de los activos

La opción Establecer privilegios de estados de los activos le permiten establecer el estado de un recurso en Activo o Retirado.

Las soluciones instaladas en Symantec Management Platform pueden agregar más privilegios a esta categoría. Por ejemplo, Asset Management Solution agrega tres o cuatro privilegios aquí.

Ver "Categorías de privilegios de seguridad" en la página 489.

Ver "Asignación de privilegios a un rol de seguridad" en la página 93.

Tabla A-14 Establecer privilegios de estados de los activos

Privilegio	Descripción	Tipos de elementos a los que se aplica	Requisitos adicionales
Activo	Determina el estado del recurso seleccionado como Activo.	Solamente recursos	Permiso de escritura en el grupo organizativo que contiene el recurso.
Retirado	Determina el estado del recurso seleccionado como Retirado.	Solamente recursos	Permiso de escritura en el grupo organizativo que contiene el recurso.

Permisos de administración de recursos

Estos permisos se aplican a recursos.

Ver "Categorías de permisos de seguridad" en la página 491.

Tabla A-15 Permisos de administración de recursos

Permiso	Descripción
Leer datos de recursos	Le permite leer datos de recursos.
Leer asociación de recursos	Le permite leer datos de asociación de recursos.
Escribir datos de recursos	Le permite escribir datos de recursos.
Escribir asociación de recursos	Le permite escribir datos de asociación de recursos.

Permisos del sistema

Estos permisos se aplican al sistema, como la lectura, la escritura y la eliminación de elementos.

Ver "Categorías de permisos de seguridad" en la página 491.

Tabla A-16 Permisos del sistema

Permiso	Descripción
Control completo	Le permite tomar control completo sobre un elemento que posee otro usuario. Ver "Propiedad de una carpeta o elemento" en la página 115.
Eliminar	Le permite eliminar elementos.
Escribir	Le permite crear o modificar elementos.
Clonar	Le permite clonar un elemento existente.
Leer	Le permite abrir un elemento y ver los contenidos de los elementos.
Cambiar permisos	Le permite cambiar los permisos en los elementos.
Leer permisos	Le permite leer los permisos para un elemento.

Permisos de Task Server

Estos permisos se aplican a Task Server.

Ver "Categorías de permisos de seguridad" en la página 491.

Tabla A-17 Permisos de Task Server

Permiso	Descripción
Crear una nueva tarea	Le permite crear tareas nuevas.
Ejecutar script	Le permite ejecutar un script.
Ejecutar Control de energía	Le permite ejecutar tareas de control de energía.
Ejecutar tarea	Le permite ejecutar tareas.
Ejecutar Controlar estado de servicio	Le permite ejecutar una tarea para controlar el estado del servicio.

Permisos de informes

Estos permisos se aplican a los informes.

Ver "Categorías de permisos de seguridad" en la página 491.

Tabla A-18 Permisos de informes

Permiso	Descripción
Ejecutar informes	Le permite ejecutar un informe.
Guardar informes	Le permite guardar un informe.

Permisos de políticas

Estos permisos se aplican a las políticas.

Ver "Categorías de permisos de seguridad" en la página 491.

Tabla A-19 Permisos de políticas

Permiso	Descripción
Aplicar a destinos de recursos	Permite aplicar los destinos de recursos a las políticas.
Habilitar la política	Permite habilitar o deshabilitar una política.

Permisos de carpeta

Estos permisos se aplican a las carpetas.

Ver "Categorías de permisos de seguridad" en la página 491.

Tabla A-20 Permisos de carpeta

Permiso	Descripción
Crear secundarios	Le permite agregar elementos y subcarpetas a una carpeta.

Permisos de filtro

Estos permisos se aplican a los filtros.

Ver "Categorías de permisos de seguridad" en la página 491.

Tabla A-21 Permisos de filtro

Permiso	Descripción
Aplicar configuración del agente	Le permite cambiar una política de configuración del agente de destino y aplicarla a un destino de recurso.
Aplicar tareas de Software Delivery	Le permite aplicar tareas de entrega de software.

Permisos del perfil de conexión

Estos permisos le permiten usar perfiles de conexión. Los perfiles de conexión almacenan la información necesaria para comunicarse con los equipos y otros dispositivos de red mediante los protocolos de red estándar de supervisión. Estos protocolos incluyen SNMP, WMI, WSMan y otros.

Ver "Categorías de permisos de seguridad" en la página 491.

Los perfiles de conexión se asocian a los dispositivos durante la detección de red. Durante la detección, se selecciona un perfil de conexión para definir los protocolos y las credenciales que se deben usar. Cuando la detección finaliza, este perfil de conexión se asocia a cada recurso detectado. Cuando la información se requiere, el perfil de conexión asociado se usa para conectarse.

Tabla A-22 Permisos del perfil de conexión

Permiso	Descripción
Uso	Le permite usar perfiles de conexión.

Permisos de Credential Manager

Credential Manager proporciona una ubicación segura de almacenamiento para los nombres de usuario y las contraseñas. Las soluciones que están instaladas en Symantec Management Platform definen los tipos de credenciales que Credential Manager almacena. Estos permisos le permiten usar Credential Manager.

Ver "Categorías de permisos de seguridad" en la página 491.

Tabla A-23 Permisos de Credential Manager

Permiso	Descripción
Uso	Le permite usar Credential Manager.

Apéndice B

Symantec Management Agent

En este Apéndice se incluyen los temas siguientes:

- Intervalos de actualización de datos recomendados de Symantec Management Agent
- Comandos de solución de problemas de Symantec Management Agent para UNIX, Linux y Mac

Intervalos de actualización de datos recomendados de Symantec Management Agent

Symantec Management Agent regularmente envía datos de inventario básicos a Notification Server y recibe de este datos de configuración del agente. Puede configurar los intervalos de las actualizaciones. Cuantos más equipos administre, menos frecuentemente tendrá que actualizar los datos a fin de reducir la carga de Notification Server.

Ver "Configuración de las opciones de configuración del agente de destino" en la página 278.

Tabla B-1 Intervalos de actualización de datos recomendados de Symantec Management Agent

Cantidad de equipos administrados	Inventario básico	Solicitud de configuración
0 - 499	30 minutos.	15 minutos.
500 - 1999	8 horas	4 horas

Cantidad de equipos administrados	Inventario básico	Solicitud de configuración
> 2000	24 horas	8 horas

Notification Server incluye una política de automatización que automáticamente le envía un correo electrónico cuando los intervalos de actualización son menores que los valores recomendados. La política Verificación de escalabilidad evita tener que comprobar los intervalos de actualización cada vez que se agregan o eliminan equipos en la red. Puede encender o apagar la política Verificación de escalabilidad según sea necesario, y establecer la programación apropiada.

Ver "Administración de políticas de automatización" en la página 393.

Comandos de solución de problemas de Symantec Management Agent para UNIX, Linux y Mac

Es posible usar comandos para la resolución de problemas. Se deben ejecutar dentro de una ventana de comandos en el sistema de destino. A menos que se especifiquen los nombres de ruta completa, ejecute estos comandos desde el directorio local donde reside la binaria. Las ubicaciones de ruta binarias se especifican con cada comando.

Nota: El directorio de instalación del agente predeterminado para Symantec Management Agent es **/opt/altiris/notification/nsagent**. Es posible modificarlo en Symantec Management Console, en **Configuración > Configuración de instalación > Configuración del agente**.

Ver "Cómo instalar Symantec Management Agent para UNIX, Linux y Mac manualmente en modo push" en la página 260.

Tabla B-2 Comandos de Symantec Management Agent

Propósito	Comando de /opt/altiris/notification/nsagent/bin
Forzar una actualización de política.	`aex-refreshpolicies`
Enviar inventario básico.	`aex-sendbasicinv`
Consultar las tareas disponibles del paquete de software con la opción para ejecutarlas manualmente.	`aex-swdapm`

Propósito	Comando de /opt/altiris/notification/nsagent/bin
Desinstalar manualmente el agente.	`aex-uninstall`
Reiniciar el agente.	`aex-helper agent restart`

Client Task Agent puede mostrar información acerca de cualquier tarea que haya sido asignada al cliente UNIX/Linux. La tabla siguiente detalla los comandos útiles para Client Task Agent.

Tabla B-3 Comandos de Client Task Agent

Propósito	Ejecute este comando desde /opt/altiris/notification/ctagent/bin
Abrir la ayuda en un comando.	`aex-cta help`
Enumerar las tareas actuales y sus instancias de ejecución.	`aex-cta list`
Enumerar las tareas que se ejecutan en el cliente y su GUID.	`aex-cta list --show-task-id`
Enumerar tareas pendientes.	`aex-cta pending`
Actualizar la configuración de agente.	`aex-cta refresh`
Forzar el registro de nuevo con Task Server.	`aex-cta register`
Obtener información sobre Task Server actualmente registrado.	`aex-cta ts`
Comprobar que el agente se está ejecutando.	`aex-helper check`
Recuperar una lista de las políticas de implementación administrada que se ejecutan.	`aex-cta list`

Propósito	Ejecute este comando desde /opt/altiris/notification/ctagent/bin
Recuperar una lista de las políticas de implementación administrada y de las tareas de Entrega rápida que se ejecutan en el cliente.	`aex-cta list --show-all-tasks`
Enumerar tareas de instalación de complementos.	`aex-smf list`
Permitir el aplazamiento de la ejecución de tareas en el cliente según la configuración de tareas.	`aex-swd-defer`

Tabla B-4 Comandos de administración de software

Propósito	Ejecute este comando desde /opt/altiris/notification/smfagent/bin
Mostrar trabajos de administración de software y su estado.	`aex-smf list`

La tabla siguiente detalla los comandos `aex-helper`. `aex-helper` es una utilidad del cliente para ayudar a solucionar problemas y acelerar las tareas de administrador.

La sintaxis para la utilidad es `aex-helper [opciones de comando]`

Tabla B-5 Comandos `Aex-helper`

Propósito	Comando desde /opt/altiris/notification/nsagent/bin
Registrar dependencias entre las soluciones.	`adddep`
Realizar diversas tareas con el agente de UNIX.	`agent`
Cambiar las propiedades de los servicios registrados de RC.	`changerc`
Comprobar que Symantec Management Agent para UNIX, Linux y Mac se está ejecutando.	`check`

Propósito	Comando desde /opt/altiris/notification/nsagent/bin
Limpiar los elementos del registro XML.	`clean`
Mostrar la ayuda sobre el comando especificado.	`help`
Consultar con el agente diferentes datos.	`info`
Instalar y registrar los scripts de RC.	`installrc`
Trabajar con el marco de IPC del agente.	`ipc`
Crear scripts y vínculos de ajustador para las bibliotecas y los archivos ejecutables.	`link`
Enumerar objetos en el registro del agente.	`list`
Consultar con el agente diferentes datos.	`query`
Iniciar, detener y detallar los servicios registrados de RC.	`rc`
Agregar un objeto al registro del agente.	`register`
Desinstalar soluciones.	`uninstall`
Desinstalar scripts de RC.	`uninstallrc`
Quitar scripts y vínculos de ajustador para las bibliotecas y los archivos ejecutables.	`unlink`
Quite objetos del registro del agente.	`unregister`
Actualizar el complemento de Symantec Management Agent.	`upgrade`

Puede también usar un archivo de registro del cliente para ayudar a solucionar problemas. Para solucionar problemas usando este archivo de registro, use los comandos en la tabla siguiente.

Tabla B-6 Comandos del archivo de registro

Propósito	Comando desde /opt/altiris/notification/nsagent/var
Aumentar el nivel de registro al estado de depuración.	`aex-helper agent -s Configuration debug_level debug`

Propósito	Comando desde /opt/altiris/notification/nsagent/var
Desactivar el límite de tamaño del registro.	`aex-helper agent -s Configuration debug_file_size 0`
Regresar parámetros a su estado predeterminado.	`aex-helper agent -s Configuration debug_level error` `aex-helper agent -s Configuration debug_file_size 1024`

Apéndice C

Temas de referencia de administración habilitada para la nube

En este Apéndice se incluyen los temas siguientes:

- Herramientas de la línea de comandos de Notification Server
- Configuraciones admitidas para los servidores de paquetes en un entorno mixto
- Efectos de la funcionalidad Administración habilitada para la nube en el servidor de sitio
- Scripts de administración del gateway de Internet
- Acerca del equilibrio de carga del gateway de Internet
- Parámetros del paquete de instalación del agente habilitado para la nube
- Conmutadores de línea de comandos para la configuración de agentes habilitados para la nube

Herramientas de la línea de comandos de Notification Server

La tabla siguiente describe las herramientas de la línea de comandos que están disponibles para uso con Notification Server. Es posible usar estas herramientas para mantener su entorno de administración habilitada para la nube.

Tabla C-1 Herramientas de la línea de comandos de Notification Server

Nombre ejecutable	Descripción
AeXGenClientCert.exe	La herramienta del generador del certificado de cliente le permite crear los certificados de cliente que necesita. El certificado de la autoridad de certificación (CA) de agente de Notification Server emite estos certificados. Ver "Cómo generar un certificado de cliente temporal" en la página 328.
AeXGenSiteServerCert.exe	La herramienta del generador del certificado de servidor le permite crear los certificados de cliente que necesita. El certificado de CA de Notification Server emite estos certificados. **Nota:** Aplicar un certificado de servidor regenerado a un gateway de Internet afecta los Symantec Management Agents existentes. Los agentes existentes no pueden conectarse al gateway de Internet hasta que reciben los detalles actualizados de la huella digital de certificado del gateway. Ver "Generar y aplicar el certificado de servidor de sitio para el acceso del agente habilitado para la nube" en la página 296.
AeXRevokeCertificate.exe	La herramienta de la revocación del certificado. Esta herramienta le permite revocar un certificado actualizando la lista de revocación del certificado (Certificate Revocation List, CRL). Ver "Revocar un certificado de administración habilitada para la nube" en la página 332.

Ver "Tareas de mantenimiento y solución de problemas habilitadas para la nube" en la página 327.

Configuraciones admitidas para los servidores de paquetes en un entorno mixto

IT Management Suite admite un entorno mixto donde algunos servidores de sitio son internos y algunos servidores de sitio son servidores de sitio de Internet. En un entorno mixto, Symantec Management Agent primero intenta usar los servidores de paquetes internos. Si ningún servidor de paquetes interno está disponible, el agente pasa a usar los servidores de paquetes de Internet que están detrás de un gateway.

Tabla C-2 Configuraciones admitidas para los servidores de paquetes en un entorno mixto

Configuración	Descripción
Defina algunos servidores de paquetes de Internet para cada sitio habilitado para la nube.	Los servidores de paquetes de Internet deben publicar sus bases de código en el formato HTTPS. Para esta configuración de sitio determinada, puede marcar todos los servidores de paquetes de Internet dentro del sitio como restringidos. Esta configuración garantiza que los servidores de paquetes de Internet descarguen los paquetes solamente de servidores de paquetes internos específicos dentro de su propio sitio. Si un servidor de paquetes de Internet dentro del sitio descarga un paquete por medio de Internet, el paquete se vuelve disponible para otros servidores de paquetes de Internet dentro de ese sitio. A continuación los otros servidores de paquetes pueden descargar el paquete del servidor de paquetes que está en la misma subred en lugar de descargar el paquete a través de Internet. Si no hay servidores de paquetes internos asignados al sitio, por lo menos un servidor de paquetes de Internet debe estar disponible dentro del sitio. Esta configuración garantiza que al menos un Package Server pueda proporcionar paquetes fuera de su sitio para la distribución dentro de su propio sitio. Ver "Configuración de un servidor de paquetes para publicar bases de código de paquetes de HTTPS" en la página 302.
Configure Notification Server de modo que requiera SSL.	Esta configuración hace que Notification Server publique las bases de código de HTTPS, lo que permite a los servidores de paquetes y a los agentes habilitados para la nube descargar paquetes de Notification Server. Sin embargo, esto significa que todos los clientes internos (directamente administrados) tendrán que comunicarse con Notification Server mediante HTTPS, una opción que probablemente no desee. Ver "Configurar Notification Server para usar HTTPS" en la página 291. **Nota:** Notification Server no puede publicar las bases de código HTTP y HTTPS al mismo tiempo.

Efectos de la funcionalidad Administración habilitada para la nube en el servidor de sitio

La administración habilitada para la nube tiene los siguientes efectos sobre funcionalidad del servidor de paquetes y Task Server:

Tabla C-3 Efectos de la funcionalidad Administración habilitada para la nube en el servidor de sitio

Efecto	Descripción
Los servidores de paquetes en la red interna entregan paquetes a los agentes habilitados para la nube y a los servidores de paquetes mediante HTTPS únicamente.	Sin embargo, los servidores de paquetes de la red interna aún pueden descargar paquetes en clientes de la red interna mediante UNC o HTTP. Del mismo modo, los servidores de paquetes desconectados en el sitio local pueden entregar paquetes a los clientes habilitados para la nube en el mismo sitio local mediante cualquier protocolo.
El proceso de selección del servidor en los servidores de paquetes y los agentes habilitados para la nube no es el mismo.	El proceso de selección del servidor en los servidores de paquetes y los agentes habilitados para la nube es el siguiente: Los orígenes de servidores de paquetes que están disponibles para el servidor de paquetes o el agente habilitado para la nube típicamente incluyen servidores de paquetes locales y servidores de paquetes de la red interna. De forma predeterminada, el agente elige una opción de la lista de Package Servers locales. El agente usa los Package Servers de la red interna solamente en las situaciones siguientes: Todos los Package Servers locales tienen perfil de velocidad 0 o se registran más de siete errores.
Se deben realizar actividades adicionales cuando se elimina un servidor de paquetes.	Si elimina un servidor de paquetes de un equipo que está agregado al gateway de Internet, por razones de seguridad, también se debe eliminar el servidor de paquetes del gateway de Internet.
Un Task Server remoto no se puede instalar en un equipo cliente que ya tenga una política de **Configuración de administración habilitada para la nube** aplicada.	Sin embargo, la política de **Configuración de administración habilitada para la nube** se puede aplicar al equipo cliente una vez que el Task Server está instalado.
Los Task Servers no pueden proporcionar notificaciones en tiempo real o entrega de tareas en tiempo real.	El sondeo periódico es el modo admitido para ejecutar tareas en clientes habilitados para la nube. De forma predeterminada, Symantec Management Agent comprueba la existencia de tareas cada 30 minutos. Puede cambiar esta configuración para los agentes habilitados para la nube mediante la modificación de la configuración **Actualización de tarea** en la política **Configuración del agente de tareas**. Esta página de políticas está disponible en Symantec Management Console, en **Configuración > Notification Server > Configuración de tareas**. Ver "Cómo cambiar la configuración de Client Task Agent" en la página 430.
La prueba de velocidad de Task Servers se reemplaza con clasificación aleatoria.	El Agente de tareas del cliente ordena aleatoriamente la lista de Task Servers en situaciones donde, de lo contrario, se usaría el orden basado en prueba de velocidad. Tenga en cuenta que el agente omite la prueba de velocidad solamente cuando está en modo habilitado para la nube.

Efecto	Descripción
De forma predeterminada, los Task Servers funcionan con los agentes locales y habilitados para la nube.	Los Task Servers asignados al sitio de Internet trabajan con los agentes ubicados en la intranet y los agentes habilitados para la nube. Para forzar los agentes habilitados para la nube a comunicarse con el Task Server seleccionado, asigne manualmente esos agentes a un Task Server específico. Ver "Cómo administrar agentes asignados de forma manual" en la página 134.

Scripts de administración del gateway de Internet

Para ayudarlo a administrar y mantener sus gateways de Internet, varios scripts están disponibles en el directorio de instalación del gateway de Internet de Symantec Management Platform.

Tabla C-4 Scripts de administración del gateway de Internet

Ubicación y nombre del script	Descripción
`Apache\bin\GenerateCert.cmd`	Regenera el certificado de servidor.
`Apache\certs\client\UpdateCertHashes.cmd`	Aplica un certificado de la autoridad de certificación (CA) de Notification Server al gateway de Internet.
`Apache\certs\crl\UpdateCrlHashes.cmd`	Aplica una Lista de revocación de certificados (CRL) al gateway de Internet. Ver "Revocar un certificado de administración habilitada para la nube" en la página 332.
`Apache\bin\StartService.cmd`	Inicia el servicio de gateway de Internet.
`Apache\bin\StopService.cmd`	Detiene el servicio de gateway de Internet.
`Apache\bin\InstallService.cmd`	Registra (o vuelve a registrar) el servicio de gateway de Internet en los servicios de Windows.
`Apache\bin\UninstallService.cmd`	Anula el registro del servicio de gateway de Internet de los servicios de Windows.

Ver "Tareas de mantenimiento y solución de problemas habilitadas para la nube" en la página 327.

Acerca del equilibrio de carga del gateway de Internet

El gateway de Internet puede aceptar 3000 conexiones simultáneas y puede admitir de 1 a 60 000 endpoints. El número máximo de clientes que un gateway de Internet puede servir depende del entorno. Por ejemplo, intervalos de solicitud de tarea y políticas más breves implican una mayor recepción de solicitudes por parte del gateway. Un número elevado de solicitudes reduce la cantidad de clientes que el gateway puede admitir. Otra variable es el período de conexión que los agentes necesitan. En la mayoría de los casos, el agente se conecta solamente por un tiempo breve. Sin embargo, cuando el agente descarga paquetes o el inventario de informes, una conexión puede durar un período mucho más prolongado.

En Symantec Management Platform, los gateways de Internet que tienen problemas de conexión no se marcan como defectuosos y se omiten. En cada transferencia, Symantec Management Agent prueba todos los gateways de la lista hasta que encuentra uno que funciona. En función de la naturaleza de los problemas que causan los errores de gateway, es posible que un gateway determinado se sobrecargue. El sistema se balancea eventualmente de manera correcta sin intervención manual.

Los gateways de Internet no admiten ningún balanceo de carga manual configurable. Todos los balanceos de carga se hacen automáticamente.

Un agente habilitado para la nube realiza el equilibrio de carga de la siguiente manera:

- Symantec Management Agent selecciona aleatoriamente un gateway de Internet de la lista de gateways disponibles que se especifican en la política **Configuración de Administración habilitada para la nube**. El agente entonces usa el gateway seleccionado hasta que la conexión falle.
  La selección es siempre aleatoria, todos los gateways se consideran iguales, y no puede asignar una preferencia o una carga a ningún gateway determinado.
- Cuando el agente no puede conectarse por medio del gateway preferido, selecciona aleatoriamente otro gateway de la lista. El agente usa ese gateway para todas las conexiones hasta que también falle.
- Periódicamente, al doble del intervalo de elaboración de informes de inventario básico, el agente restablece su selección al seleccionar aleatoriamente un gateway de la lista de gateways disponibles.

Este proceso asegura que si un nuevo gateway se agrega al sistema, la carga de conexión pronto se rebalancee automáticamente. El mismo rebalanceo automático ocurre si un gateway tiene un problema temporal y se desconecta.

Ver "Configurar la administración habilitada para la nube" en la página 307.

Ver "Acerca de la preparación del equipo de gateway de Internet" en la página 313.

Parámetros del paquete de instalación del agente habilitado para la nube

Es posible generar un paquete de instalación de Symantec Management Agent desde Symantec Management Console. Es necesario generar el paquete en la instancia de Symantec Management Platform que administra el agente instalado. El paquete de instalación generado contiene el instalador de Symantec Management Agent para la plataforma apropiada. El paquete además contiene los certificados que el cliente necesita para confiar en Notification Server.

Cuando genera un paquete de instalación del agente, es necesario especificar los parámetros apropiados del paquete.

Tabla C-5 Parámetros del paquete de instalación de Symantec Management Agent

Parámetro	Descripción
Sistema operativo	El sistema operativo en el equipo cliente. **Nota:** Solamente se admiten clientes de Microsoft Windows en Symantec Management Platform 7.5.
Política	La lista desplegable contiene todas las políticas de administración habilitadas para la nube que están habilitadas actualmente. Es necesario seleccionar la política de configuración de la administración habilitada para la nube que aplica a este agente habilitado para la nube. La política seleccionada especifica los gateways de Internet disponibles que el agente recientemente instalado puede usar. La lista de gateways disponibles se incluye con el paquete de instalación de Symantec Management Agent. Ver "Configurar la política de Configuración de administración habilitada para la nube " en la página 320.
Grupo organizativo	El grupo organizativo al que pertenece el equipo habilitado para la nube. Esta configuración es opcional. Si selecciona un grupo organizativo, el agente recientemente instalado se asigna automáticamente al grupo organizativo especificado cuando el equipo se encuentra bajo administración. Es necesario usar un grupo organizativo que ha creado. No elija grupos organizativos predeterminados. Estos grupos se basan en tipos de recursos y no son convenientes para equipos habilitados para la nube. Por ejemplo, un proveedor de servicios administrados (MSP) puede tener varios clientes y administrar cada uno de ellos con un grupo organizativo específico del cliente. Esta configuración permite a cada equipo recientemente instalado asignarse automáticamente al grupo organizativo apropiado.

Parámetro	Descripción
Nombre de instalación	Un nombre de paquete de instalación fácil para el usuario. Este nombre se muestra en la línea de asunto del certificado de Symantec Management Agent que se conecta al instalador. Este nombre se puede usar con fines de informe y diagnóstico. Para la instalación de un solo equipo, es posible que desee usar el nombre del usuario principal o del equipo. Para un paquete que está instalado en varios equipos, es conveniente usar el identificador apropiado de oficina o de departamento.
Caducidad	La fecha y la hora en que caduca el paquete de instalación. La opción predeterminada es siete días después de la fecha de creación. Es necesario especificar una fecha que sea al menos un día posterior a la fecha (de creación) actual.
Distribución automatizada de certificados	Define si el certificado permanente de un agente se emite de forma automática. Si no se lo emite automáticamente, un administrador tiene que administrar la distribución del certificado y necesita autorizar cada solicitud de la sección de informes de Notification Server.
Limitar cantidad de registros de agente	Define cuántas veces se puede emitir un certificado permanente. El certificado se emite en función del número de solicitudes que se envíen usando un certificado de sitio o un certificado temporal.
Firmar mediante	Además tiene la opción de agregar una firma al paquete de instalación. Es posible elegir entre firmar con una contraseña o firmar con una huella digital.

Conmutadores de línea de comandos para la configuración de agentes habilitados para la nube

Es posible usar los conmutadores de línea de comandos para configurar la administración habilitada para la nube en Symantec Management Agent.

Nota: Una vez que se usan los conmutadores de línea de comandos, es necesario reiniciar Symantec Management Agent para que la configuración surta efecto.

Tabla C-6 Conmutadores de línea de comandos `AeXNSAgent.exe`

Conmutador de línea de comandos	Descripción
`/gw=gatewayName,port,thumbprint`	Especifica un gateway de Internet que Symantec Management Agent puede usar. Ver "Cómo forzar Symantec Management Agent para usar un gateway de Internet especificado" en la página 335.

Conmutador de línea de comandos	Descripción
`/importcert=certificateFile.pfx`	Agrega un certificado especificado a la configuración de Symantec Management Agent. Este comando coloca el certificado en el almacén de certificados del servicio de Symantec Management Agent. Además agrega la huella digital de certificado al registro. Ver "Cómo instalar un certificado temporal en un equipo administrado" en la página 331.
`/removecert`	Elimina el certificado actual de la configuración de Symantec Management Agent. Este comando elimina el certificado del agente del almacén de certificados del servicio de Symantec Management Agent. Además elimina la huella digital de certificado del registro. Ver "Cómo instalar un certificado temporal en un equipo administrado" en la página 331.
`/rootca=certificateFile.cer`	Agrega un certificado de la autoridad de certificación (CA) raíz. Este comando inserta el certificado especificado en el almacén de certificados de **Autoridades de certificación raíz de confianza**. Ver "Cómo aplicar un certificado de una autoridad de certificación raíz a un equipo administrado" en la página 292.
`/cem=on`	Habilita la administración habilitada para la nube Symantec Management Agent activando la comunicación segura.
`/cem=off`	Deshabilita la administración habilitada para la nube en Symantec Management Agent desactivando la comunicación segura.
`/clearcem`	Borra toda la configuración de la administración habilitada para la nube de la configuración de Symantec Management Agent.

Ver "Tareas de mantenimiento y solución de problemas habilitadas para la nube" en la página 327.

Apéndice D

Configuración del informe personalizado

En este Apéndice se incluyen los temas siguientes:

- Página Edición de informes personalizada
- Página Edición de informes personalizada: Ficha Origen de datos
- Página Edición de informes personalizada: ficha Origen de datos, ficha Consulta
- Página Edición de informes personalizada: ficha Origen de datos, ficha: Campos
- Página Edición de informes personalizada: ficha Origen de datos, ficha Consulta con parámetros
- Página Edición de informes personalizada: ficha Origen de datos, ficha Parámetros de consulta
- Página Edición de informes personalizada: ficha Origen de datos, ficha: Expresiones de filtro
- El informe personalizado edita la página: ficha Origen de datos : ficha Instantáneas de datos
- Página Edición de informes personalizada: ficha Origen de datos,, ficha: Consulta resuelta
- Página Edición de informes personalizada: ficha Origen de datos, ficha Resultados
- Página Edición de informes personalizada: ficha Vistas para una vista de gráfico
- Página Edición de informes personalizada: ficha Vistas para una vista de cuadrícula

- Cuadro de diálogo Editar campos de origen
- Cuadro de diálogo Edición de parámetro

Página Edición de informes personalizada

La página **Edición de informes personalizada** permite definir y editar los componentes y las propiedades del informe personalizado de Notification Server que se crea o se modifica.

Ver "Componentes de un informe personalizado de Notification Server" en la página 450.

Ver "Creación y modificación de informes personalizados de Notification Server" en la página 452.

Tabla D-1 Fichas de la página Edición de informes personalizada

Ficha	Descripción
Origen de datos	Permite definir la consulta del informe. Puede escribir la consulta SQL usted mismo o usar la Generación de consultas para generar la consulta de informe. Ver "Cómo definir una consulta de recursos para un informe personalizado" en la página 457. Ver "Cómo definir una consulta SQL para un informe personalizado" en la página 459. Ver "Página Edición de informes personalizada: Ficha Origen de datos " en la página 527.
Vistas	Permite definir vistas del informe. Una vista de informe es una manera determinada en la que se visualizan los resultados del informe. Ver "Cómo crear o modificar una vista de gráfico para un informe personalizado" en la página 462. Ver "Cómo crear o modificar una vista de cuadrícula para un informe personalizado" en la página 464. Ver "Página Edición de informes personalizada: ficha Vistas para una vista de gráfico" en la página 539. Ver "Página Edición de informes personalizada: ficha Vistas para una vista de cuadrícula" en la página 542.

Ficha	Descripción
Parámetros de informe	Permite definir parámetros de informe y proveedores de valor. Ver "Definir parámetros y proveedores de valores para un informe personalizado" en la página 460.
Examinaciones de niveles inferiores	Permite configurar las acciones de examinar niveles inferiores de un informe. Ver "Cómo configurar acciones de examinación de niveles inferiores para un informe personalizado" en la página 465.
Opciones avanzadas	Permite especificar las propiedades de un informe. Ver "Cómo especificar las propiedades avanzadas de un informe personalizado" en la página 468.

Página Edición de informes personalizada: Ficha Origen de datos

La ficha **Origen de datos** permite especificar los detalles de la consulta para un informe personalizado de Notification Server que se crea o se modifica. La vista de la ficha **Origen de datos** depende del tipo de consulta de informe que define y puede contener las fichas siguientes:

Para una consulta de recursos	Consulte Tabla D-2.
Para una consulta SQL	Consulte Tabla D-3.

Ver "Página Edición de informes personalizada" en la página 526.

Ver "Cómo definir una consulta de recursos para un informe personalizado" en la página 457.

Ver "Cómo definir una consulta SQL para un informe personalizado" en la página 459.

Si está editando una consulta de recursos, la ficha **Origen de datos** contiene el botón **Convertir esta consulta en una Consulta SQL** que permite convertir una consulta de recursos en una consulta SQL equivalente. Cuando convierte una consulta de recursos en una consulta SQL, la vista de las fichas en la ficha **Origen de datos** cambia de forma automática.

Tabla D-2 Fichas de la ficha **Origen de datos** para una consulta de recursos

Ficha	Descripción
Consulta	Permite generar una consulta de recursos y definir la sintaxis de consulta de recursos. Ver "Página Edición de informes personalizada: ficha Origen de datos, ficha Consulta " en la página 529.
Campos	Permite definir campos de origen para usar en la consulta. Es posible seleccionar la tabla de la base de datos (Origen) y la columna (Campo) que desea extraer de la CMDB. Es posible especificar si se muestra cada campo de origen en los resultados del informe. Es posible también configurar el orden de la columna y la agrupación de filas del campo de origen en la cuadrícula de resultados del informe. Ver "Página Edición de informes personalizada: ficha Origen de datos, ficha: Campos " en la página 532.
Parámetros de consulta	Permite especificar los parámetros que se usan en la consulta. Estos son parámetros internos para uso de SQL. Ver "Página Edición de informes personalizada: ficha Origen de datos, ficha Parámetros de consulta " en la página 534.
Expresiones de filtro	Permite configurar las instrucciones condicionales que se usan para acotar los resultados de la consulta. Cada instrucción o instrucción agrupada se puede considerar un filtro. Es necesario crear las instrucciones que desee usar y agruparlas como corresponda. Ver "Página Edición de informes personalizada: ficha Origen de datos, ficha: Expresiones de filtro " en la página 535.
Consulta resuelta	Permite consultar el código SQL que se ejecuta en CMDB para extraer los resultados del informe. Este código incluye los valores de prueba predeterminados para cualquier parámetro que el usuario especifique. Ver "Página Edición de informes personalizada: ficha Origen de datos,, ficha: Consulta resuelta " en la página 537.
Resultados	Permite ver los resultados de la consulta. Ver "Página Edición de informes personalizada: ficha Origen de datos, ficha Resultados " en la página 538.

Tabla D-3 Fichas de la ficha **Origen de datos** para una consulta SQL

Ficha	Descripción
Consulta con parámetros	Permite escribir el código SQL para la consulta. Este código puede incluir algunos parámetros que usan valores definidos por el usuario cuando la consulta se ejecuta en la CMDB. Ver "Página Edición de informes personalizada: ficha Origen de datos, ficha Consulta con parámetros " en la página 533.
Parámetros de consulta	Permite especificar los parámetros que se usan en la consulta. Estos son parámetros internos para uso de SQL. Ver "Página Edición de informes personalizada: ficha Origen de datos, ficha Parámetros de consulta " en la página 534.
Instantáneas de datos	Especifican los campos GUID de determinación del ámbito que se usan para determinar el ámbito de los datos que se cargan a partir de una instantánea de informe. Los datos se visualizan como los resultados del informe y poseen un ámbito determinado en función de los permisos de seguridad del usuario. Ver "El informe personalizado edita la página: ficha Origen de datos : ficha Instantáneas de datos " en la página 535.
Consulta resuelta	Permite consultar el código SQL que se ejecuta en CMDB para extraer los resultados del informe. Este código incluye los valores de prueba predeterminados para cualquier parámetro que el usuario pueda configurar. Ver "Página Edición de informes personalizada: ficha Origen de datos,, ficha: Consulta resuelta " en la página 537.
Resultados	Permite ver los resultados de la consulta. Ver "Página Edición de informes personalizada: ficha Origen de datos, ficha Resultados " en la página 538.

Página Edición de informes personalizada: ficha Origen de datos, ficha Consulta

Cuando define una consulta de recursos para informes o filtros personalizados, es necesario generar una consulta de recursos en la ficha **Consulta**.

Ver "Cómo definir una consulta de recursos para un informe personalizado" en la página 457.

Ver "Cómo definir una consulta de recursos para un filtro" en la página 358.

La ficha **Consulta** permite generar una consulta de recursos. La plantilla estándar incluye una consulta base que selecciona todos los recursos. Es posible usar la Generación de consultas para restringir la consulta base mediante los bloques de creación proporcionados. No es necesario comprender ni escribir ningún código SQL.

El panel izquierdo de la Generación de consultas muestra la estructura de la consulta. El panel derecho permite agregar y modificar elementos en la estructura de la consulta. La Generación de consultas permite generar la consulta a partir de la estructura del recurso (las clases, los tipos y las asociaciones de recursos) que se define en la CMDB. La consulta de recursos se convierte en código SQL en segundo plano. Es posible ver el código SQL en la ficha **Consulta resuelta**.

Tabla D-4 Opciones de la ficha **Consulta**

Opción	Descripción
Tipo de recurso	Le permite cambiar el tipo de recurso básico. Si creó el informe como un informe de equipo o un informe de usuario, el tipo de recurso básico se configura automáticamente en **Equipo** o **Usuario**.
Alias	El alias del tipo de recurso. El alias permite sustituir el nombre de la tabla por otro diferente. Por ejemplo, cuando la misma tabla se usa en varias épocas se une.
Ámbito establecido	Especifica si los resultados de la consulta tienen o no un ámbito establecido según el rol del usuario que ejecuta la consulta.
Utilizar campos y atributos de clase de datos	Permite agregar campos a la consulta. Puede seleccionar campos de la clase de datos (tales como Resource.Name o Resource.CreatedDate). Alternativamente, puede seleccionar campos de otras tablas (por ejemplo, el campo Dominio de la tabla Inv_AeX_AC_Identification). La ficha **Campos** muestra los campos que se definen en el conjunto de resultados de la consulta y permite configurar su aspecto en la cuadrícula de resultados. Ver "Página Edición de informes personalizada: ficha Origen de datos, ficha: Campos " en la página 532.

Opción	Descripción
Utilizar asociaciones de tipos de recursos	Permite agregar asociaciones de recursos a la consulta. Estas son asociaciones predefinidas entre dos tipos de recursos de Notification Server (como la asociación Usuario del equipo que vincula un equipo con un usuario). Puede ver la lista de asociaciones de tipos de recursos predefinidos disponibles en la carpeta Configuración que se encuentra en el panel izquierdo. Por ejemplo, haga clic en **Configuración > Notification Server > Configuración de recursos y clases de datos > Asociaciones de recursos**.
Crear uniones	Permite agregar uniones a la consulta. Una unión combina registros procedentes de dos tablas de CMDB diferentes. La lista desplegable **Uniones** le permite seleccionar el tipo de unión: ■ **Cruzada** Devuelve el producto de cartesiano de los conjuntos de registros de las dos tablas unidas. ■ **Exterior completa** Combina los resultados de las uniones externas izquierda y derecha. La tabla unida contiene todos los registros de ambas tablas y completa los valores NULOS para cualquier coincidencia inexistente en ambas. ■ **Interna** Necesita que cada registro en las dos tablas unidas tenga un registro coincidente. ■ **Exterior izquierda** Una unión entre dos tablas (A y B) en la que la tabla unida contiene siempre todos los registros de la tabla "izquierda" (A), incluso si la condición de unión no encuentra ningún registro coincidente en la tabla "derecha" (B). ■ **Exterior derecha** El inverso de la unión externa izquierda. Cada registro de la tabla "derecha" (B) aparecerá en la tabla unida por lo menos una vez. La siguiente lista desplegable le permite seleccionar la tabla de base de datos que desee usar. La lista desplegable **En** le permite seleccionar la columna que desee unir.

Opción	Descripción
Agregar parámetros	Abre la ficha Parámetros de consulta, que permite especificar los parámetros que desea usar en la consulta de recursos. Un parámetro es una variable que se incluye en la consulta. Ver "Página Edición de informes personalizada: ficha Origen de datos, ficha Parámetros de consulta " en la página 534.
Agregar expresiones de filtros	Abre la ficha Expresiones de filtro. Ver "Página Edición de informes personalizada: ficha Origen de datos, ficha: Expresiones de filtro " en la página 535.

Página Edición de informes personalizada: ficha Origen de datos, ficha: Campos

Cuando define una consulta de recursos para un nuevo informe personalizado o modifica una consulta de recursos para un informe personalizado existente, puede especificar los campos de origen y los atributos de clase de datos que extrae la consulta de recursos.

La ficha **Campos** le permite especificar los campos de origen y los atributos de clase de datos que extrae la consulta de recursos. Los campos son columnas de tablas en la CMDB (por ejemplo, la columna Dominio de la tabla **Inv_AeX_AC_Identification**). Las clases de datos son tipos de datos específicos del tipo de recurso que seleccionó (por ejemplo, **Nombre.Equipo**).

Es posible especificar si se muestra cada campo de origen en los resultados del informe. Es posible también configurar el orden de la columna y la agrupación de filas del campo de origen en la cuadrícula de resultados del informe.

Ver "Cómo definir una consulta de recursos para un informe personalizado" en la página 457.

Ver "Página Edición de informes personalizada: Ficha Origen de datos " en la página 527.

Nota: Esta ficha se usa para las consultas de informe solamente. No es relevante para las consultas de filtro.

Ver "Cuadro de diálogo Editar campos de origen " en la página 544.

Página Edición de informes personalizada: ficha Origen de datos, ficha Consulta con parámetros

Cuando define una consulta SQL para nuevos informes o filtros personalizados, puede escribir una consulta SQL para que se ejecute en el CMD. Cuando modifica una consulta SQL para informes o filtros personalizados existentes, puede escribir una consulta SQL para que se ejecute en el CMD. La ficha **Consulta con parámetros** permite escribir la consulta SQL que desea ejecutar en la CMDB. Esta ficha es fundamentalmente un cuadro de texto sin formato que permite escribir el código SQL o pegarlo del portapapeles. El panel Explorador de objetos permite seleccionar campos de origen de la CMDB e insertarlos en la consulta. La inserción de campos de origen simplifica la escritura de la consulta.

Ver "Cómo definir una consulta SQL para un informe personalizado" en la página 459.

Se necesita el privilegio de edición de SQL para crear o modificar consultas SQL. También es necesario tener una buena comprensión de la estructura de tablas de la CMDB. Si desea aplicar un alcance determinado a los resultados de la consulta, es necesario incluir el código SQL apropiado en la consulta.

Ver "Página Edición de informes personalizada: Ficha Origen de datos " en la página 527.

Tabla D-5 Opciones de la ficha **Consulta con parámetros**

Opción	Descripción
Cuadro de texto	Le permite escribir el texto de la consulta SQL. Es posible escribir la consulta SQL desde el comienzo o pegarla del portapapeles. Si desea agregar un campo de origen en su consulta SQL, haga clic en el código SQL en la ubicación en donde desee agregar el objeto o campo especificado y, después, haga clic en **Agregar** en la línea **Objeto** o **Campo**.
Objeto	Le permite seleccionar la tabla de base de datos que desee usar.
Campo	Le permite seleccionar la columna de la tabla que desee usar.
Alias	Le permite escribir los nombres de alias para la tabla de base de datos y la columna de la tabla.

Página Edición de informes personalizada: ficha Origen de datos, ficha Parámetros de consulta

Cuando se define una consulta para nuevos informes o filtros personalizados, o se modifica una consulta de informes o filtros personalizados existentes, se pueden usar parámetros de consulta. La ficha **Parámetros de consulta** permite especificar los parámetros que desea usar en consultas de informes o de filtros. Un parámetro es una variable que se incluye en la consulta. Los valores de los parámetros de consultas de informe y de filtro se pueden definir por el sistema o se pueden extraer de otro informe. Para las consultas de informe solamente, el usuario puede configurar los valores de parámetro apropiados en la página Informe. Cuando se ejecuta la consulta, los valores de parámetro especificados se usan en el código SQL.

Ver "Cómo definir una consulta de recursos para un informe personalizado" en la página 457.

Ver "Cómo definir una consulta SQL para un informe personalizado" en la página 459.

Ver "Cómo definir una consulta de recursos para un filtro" en la página 358.

Ver "Cómo definir una consulta SQL para un filtro" en la página 360.

El uso de los parámetros en las consultas permite crear una consulta flexible. Es posible usar dicha consulta para extraer diferentes resultados mediante la inserción de los valores de parámetro apropiados. Por ejemplo, se puede crear una consulta que incluya los parámetros para el tipo de equipo informático y para el nombre del sistema operativo. Es posible ejecutar esta consulta en cualquier combinación válida de tipo de sistema y sistema operativo para extraer los resultados que desee. Como alternativa al uso de parámetros en la consulta, se pueden especificar en código los valores de los parámetros en la consulta. Luego, se debe modificar la consulta cada vez que desee usar una combinación diferente de tipo de sistema y sistema operativo. Es posible también crear varias consultas con una combinación definida diferente de tipo de sistema y sistema operativo en cada consulta.

Cuando se crea un parámetro en la ficha **Parámetros de consulta**, la declaración del parámetro apropiada se agrega automáticamente a una consulta del recurso. Sin embargo, si desea escribir una consulta SQL, es necesario agregar manualmente la declaración de parámetro apropiada al código de la consulta.

Cuando se incluye un parámetro en una consulta de informe, se puede configurar el proveedor de valores para el parámetro. Es posible especificar el tipo de proveedor de valores y los valores válidos para el parámetro. Generalmente, el proveedor de valores permite al usuario establecer el valor de parámetro apropiado cuando ejecuta el informe. El proveedor de valores de un parámetro se configura en la ficha **Parámetros de informes**.

Ver "Definir parámetros y proveedores de valores para un informe personalizado" en la página 460.

Ver "Página Edición de informes personalizada: Ficha Origen de datos " en la página 527.

Página Edición de informes personalizada: ficha Origen de datos, ficha: Expresiones de filtro

Cuando se define una consulta para nuevos informes o filtros personalizados o se modifica una consulta de informes o filtros personalizados existentes, se pueden configurar expresiones de filtro para restringir los resultados de una consulta. La ficha **Expresiones de filtro** permite especificar reglas para restringir los resultados de una consulta. Las reglas son instrucciones condicionales que filtran los resultados sin procesar de una consulta para seleccionar los recursos que desee.

Ver "Cómo definir una consulta de recursos para un informe personalizado" en la página 457.

Ver "Página Edición de informes personalizada: Ficha Origen de datos " en la página 527.

El informe personalizado edita la página: ficha Origen de datos : ficha Instantáneas de datos

Esta información es relevante para consultas de informes solamente. La ficha **Instantáneas de datos** no aparece en las consultas del filtro.

Es posible especificar los campos de determinación del ámbito en una consulta SQL para asegurarse de que las instantáneas del informe que se capturan puedan ser definidas correctamente cuando otros usuarios acceden a ellas. Los campos de determinación del ámbito son los campos GUID que se usan para lograr una determinación de datos que se extraen de una instantánea de informe. Cuando un usuario accede a una instantánea de informe, los datos se cargan desde la instantánea de acuerdo con los permisos de seguridad del usuario. Si un campo no está determinado, se cargan todos los elementos relevantes. Si se determina la amplitud de un campo, solo se cargan los elementos que el usuario que ve los datos tiene permiso para leer.

Ver "Cómo definir una consulta SQL para un informe personalizado" en la página 459.

Los campos de determinación del ámbito que se configuran en la ficha **Instantáneas de datos** se aplican solamente a la extracción de datos de las instantáneas de informe. No afectan la consulta SQL que extrae datos desde la CMDB para guardar

como instantánea de informe. Para determinar el ámbito de una consulta SQL, es necesario incluir el código SQL apropiado para extraer resultados según los permisos de seguridad del usuario que ejecuta la consulta

---

Nota: Si se determina el ámbito de una consulta SQL, cualquier instantánea de informe se guarda con el ámbito del usuario que ejecutó la consulta. Si se intenta compartir una instantánea, asegúrese de que contenga todos los datos que puedan ser relevantes para los usuarios. Es posible asegurarse de tener todos los datos ejecutando la consulta del informe como usuario que tiene acceso a todos los recursos; por ejemplo, un miembro del rol de administrador de Symantec. Se puede usar además una tarea de ejecución de informe programada para crear la instantánea apropiada: de forma predeterminada, la tarea se ejecuta en el contexto del administrador, de modo que captura la instantánea con un ámbito global.

De forma predeterminada, un nuevo informe SQL tiene `[_ItemGuid]` configurado como campo GUID de determinación del ámbito. Este campo se usa para determinar los resultados con una unión sobre una función de determinación de ámbito de la siguiente manera:

```
INNER JOIN [fnGetTrusteeScopedResources](@v1_TrusteeScope) AS [fnGTSR]

   ON ([vri2_Resource].[Guid] = [fnGTSR_3].[ResourceGuid])
```

Donde `[vri2_Resource].[Guid]` es el nombre completo del campo con el alias de `[_ItemGuid]`.

Ver "Página Edición de informes personalizada: Ficha Origen de datos " en la página 527.

Tabla D-6 Opciones en la ficha **Instantáneas de datos**

Opción	Descripción
Campos del ámbito	Le permite ver todos los campos de GUID que se incluyen en la consulta SQL. Es necesario especificar los campos GUID que se usan para la determinación del ámbito. Si crea una consulta SQL compleja que tiene varias uniones en recursos y varias aplicaciones de la función de determinación del ámbito, es necesario añadir todas las GUID de determinación del ámbito apropiadas a la lista **Campos de GUID del ámbito**.

Opción	Descripción
Consulta de instantáneas de datos	Le permite ver el código SQL que se genera cuando la instantánea necesita ser guardada o ser cargada. Antes de guardar la consulta del informe, puede verificar que el código SQL para cargar los datos de la instantánea aplique correctamente la determinación del ámbito a los resultados guardados. La consulta en el cuadro de texto se actualiza de forma automática cada vez que se modifican los campos de determinación del ámbito o cambia la selección en la lista desplegable **Modo de Consulta de instantánea de datos**. Si no actualiza de forma automática, haga clic en **Actualizar** para actualizar el código SQL mostrado.
Modo de Consulta de instantánea de datos	Le permite seleccionar el modo de consulta: ■ **Crear tabla de datos de la instantánea** Muestra el código SQL que crea la estructura de tabla de datos de la instantánea. Esta estructura no depende de la configuración de la determinación del ámbito. ■ **Guardar información de la instantánea** Muestra el código SQL que guarda los datos para todos los campos en la tabla de datos de la instantánea. La configuración de determinación del ámbito no afecta a estos datos. ■ **Cargar información de la instantánea** Muestra el código SQL que carga los datos de la tabla de datos de la instantánea y determina el ámbito según los permisos de seguridad del usuario. SQL usa campos de determinación de alcance configurados y pertenencias TrusteeScope del usuario para extraer los datos apropiados. Estos datos entonces se presentan al usuario como resultados del informe. Los campos de determinación de alcance especificados abarcan estos datos.

Página Edición de informes personalizada: ficha Origen de datos,, ficha: Consulta resuelta

Puede ver la consulta resuelta de informes o filtros personalizados que cree o modifique. La ficha Consulta resuelta muestra el código SQL que se ejecuta en la CMDB. Cualquier parámetro que se haya especificado se establece en los valores de prueba apropiados.

Ver "Cómo definir una consulta de recursos para un informe personalizado" en la página 457.

Ver "Cómo definir una consulta SQL para un informe personalizado" en la página 459.

Si visualiza una consulta de recursos, puede configurar el modo de consulta de la lista desplegable **Modo de consulta de recursos** :

Normal	Muestra la consulta resuelta predeterminada. La consulta resuelta predeterminada se genera a partir de la consulta de recursos que especificó en la Generación de consultas, sin otras adiciones.
Crear tabla de datos de la instantánea	Agrega el código SQL a la consulta que crea una tabla de datos de instantáneas para los resultados de la consulta. Se muestra la consulta modificada.
Guardar información de la instantánea	Agrega el código SQL a la consulta que guarda los resultados de la consulta en una tabla de datos de instantáneas. Se muestra la consulta modificada.
Cargar información de la instantánea	Agrega el código SQL a la consulta que extrae los resultados de la consulta de una tabla de datos de instantáneas en lugar de extraerlos de la CMDB. Se muestra la consulta modificada.

Ver "Página Edición de informes personalizada: Ficha Origen de datos " en la página 527.

Página Edición de informes personalizada: ficha Origen de datos, ficha Resultados

Es posible ver los resultados de una consulta de un informe personalizado en la ficha **Resultados**. Cuando se abre la ficha Resultados, la consulta se ejecuta automáticamente en la CMDB y se visualizan los resultados actuales. Esta capacidad permite verificar los cambios en la consulta y probar las diferentes opciones de configuración de los parámetros de consulta.

Ver "Cómo definir una consulta de recursos para un informe personalizado" en la página 457.

Ver "Cómo definir una consulta SQL para un informe personalizado" en la página 459.

Ver "Página Edición de informes personalizada: Ficha Origen de datos " en la página 527.

Página Edición de informes personalizada: ficha Vistas para una vista de gráfico

En la ficha **Vistas** para una vista de gráfico, se puede especificar la configuración en las siguientes subfichas:

Título	Permite especificar el texto del título del gráfico y la ubicación en la cual aparece. Ver Tabla D-7 en la página 540.
Leyenda	Permite especificar el texto de la leyenda del gráfico y la ubicación en la cual aparece. La leyenda es el texto descriptivo opcional que se muestra con el gráfico. Ver Tabla D-8 en la página 540.
3D	Configurar el zoom 3D permite ampliar las áreas seleccionadas del gráfico al tamaño completo de la ventana. Por ejemplo, se puede examinar un informe grande que cubre un período largo: se puede ver un período corto determinado seleccionando la parte relevante. Es posible configurar uno o ambos ejes como expandible. Ver Tabla D-9 en la página 541.
Eje X	Le permite elegir la columna de resultados que se usará como eje X en el gráfico. La ficha además permite especificar el texto del título y configurar el aspecto del eje X. Ver Tabla D-10 en la página 541.
Eje Y	Le permite elegir la columna de resultados (o las columnas) que se usará como eje Y en el gráfico. La ficha además permite especificar el texto del título y configurar el aspecto del eje Y. Para algunos tipos de gráfico, se pueden aplicar varios valores (varias columnas de resultado) en el mismo gráfico. Aparecen como varias líneas en un gráfico lineal o como una pila de diferentes colores en una barra, cada una con una etiqueta y un color de codificación. Ver Tabla D-11 en la página 541.

Ver "Cómo crear o modificar una vista de gráfico para un informe personalizado" en la página 462.

Tabla D-7 Opciones de la ficha **Título**

Opción	Descripción
Título	El principal título del gráfico. Si desea crear un título de varias líneas, use los caracteres **\n** para insertar saltos de línea en los lugares apropiados. No hay ninguna opción predeterminada configurada, de forma que el título predeterminado del gráfico es una cadena vacía.
Sugerencia sobre herramientas	El texto que aparece en la información sobre herramientas cuando el usuario desplaza el mouse sobre el título del gráfico. No hay ninguna opción predeterminada configurada.
Alineado	Le permite especificar la ubicación y la alineación del texto correspondiente al gráfico para el idioma del sistema (formato escrito).
Acople	Le permite especificar la ubicación del título en la página del gráfico.

Tabla D-8 Opciones de la ficha **Leyenda**

Opción	Descripción
Mostrar leyenda	Seleccione esta opción para mostrar la leyenda.
En área de trazado	Seleccione esta opción para mostrar la leyenda en el área de trazado. Si se anula la selección de esta opción, la leyenda aparece fuera del área de trazado.
Título	El texto de la leyenda. No hay ninguna opción predeterminada establecida, de forma que la leyenda predeterminada es una cadena vacía.
Estilo	Le permite especificar el estilo de la leyenda.
Alineado	Le permite especificar la alineación del texto de la leyenda correspondiente al gráfico.
Acople	Le permite especificar la ubicación de la leyenda en la página del gráfico.

Tabla D-9 Opciones de la ficha **3D**

Opción	Descripción
Habilitar 3D	Seleccione esta opción para habilitar el zoom 3D.
Zoom	Compruebe estas opciones para habilitar el zoom en el eje X y el eje Y, respectivamente.
Rotación	El ángulo de rotación sobre el eje X y el eje Y, respectivamente.

Tabla D-10 Opciones de la ficha **Eje X**

Opción	Descripción
Columna principal	La columna de datos para realizar trazos a lo largo del eje X. Seleccione la opción apropiada de la lista desplegable. Las opciones son las columnas de resultado que son especificadas en el informe.
Título	El texto del título del eje X.
Visible	Seleccione esta opción para visualizar el eje X.
Cuadrículas grandes	Seleccione esta opción para visualizar las líneas de cuadrícula grande del eje X.
Invertido	Seleccione esta opción para representar el eje X en orden inverso.

Tabla D-11 Opciones de la ficha **Eje Y**

Opción	Descripción
Columna principal	La columna de datos para realizar trazos en el eje Y. Seleccione la opción apropiada de la lista desplegable. Las opciones son las columnas de resultado que fueron especificadas en el informe.
Título	El texto del título del eje Y.

Opción	Descripción
Columnas apiladas	La lista de columnas que están disponibles para ser agregadas al gráfico. Seleccione las columnas que desee agregar. Esta opción se aplica solamente a los tipos de gráficos apilados, como Columna apilada, Barra apilada y Área apilada.
Visible	Seleccione esta opción para visualizar el eje Y. De forma predeterminada, esta opción está deshabilitada, de forma que el eje Y no está visible.
Cuadrículas grandes	Seleccione esta opción para visualizar las líneas de cuadrícula grande del eje Y. De forma predeterminada, esta opción está deshabilitada, de forma que las líneas de cuadrícula grande del eje Y no están visibles.
Invertido	Seleccione esta opción para representar el eje Y en orden inverso. De forma predeterminada, esta opción está deshabilitada

Página Edición de informes personalizada: ficha Vistas para una vista de cuadrícula

La ficha **Formato avanzado** le permite configurar el formato avanzado para la vista de cuadrícula del informe personalizado que se crea o se modifica.

El proceso para configurar el formato avanzado incluye crear reglas de formato para las columnas de resultados apropiadas. Para cada regla de formato, es necesario especificar el etiquetado HTML que la regla aplica a los resultados. Si la regla de formato es condicional en ciertos valores de datos, es necesario especificar las condiciones apropiadas. Por ejemplo, en un informe de espacio libre en el disco del equipo, puede aplicar la regla de formato solamente a los equipos que tienen menos que la cantidad mínima especificada de espacio libre. La regla sería condicional en el valor Espacio libre menor que la cantidad especificada.

Ver "Cómo crear o modificar una vista de cuadrícula para un informe personalizado" en la página 464.

Tabla D-12 Opciones de la ficha **Formato avanzado**

Opción	Descripción
Nombre de la regla	Le permite especificar el nombre de la regla.
Tipo de formato	Le permite especificar el tipo de formato del informe.
Se aplica a	Le permite especificar si el formato del HTML en la plantilla se aplica a la fila entera de la cuadrícula o a la columna seleccionada solamente. Se enumera cada columna de datos en los resultados del informe. Si los resultados del informe incluyen elementos, la columna Guid de elemento también está disponible. Esta columna está oculta en todas las vistas, pero se incluye en los resultados de la consulta.
Condicional	Es posible configurar instrucciones condicionales dentro de reglas de formato para aplicar las reglas solamente a valores de datos determinados. Por ejemplo, puede resaltar ciertos valores de datos en la cuadrícula o identificar valores de datos inexistentes. Si desea configurar condiciones en la regla de formato, seleccione **Condicional**. En **Condición**, se puede fijar las condiciones para la regla de formato: ■ **Columna** Especifica la columna a la cual se aplica la condición. Se muestran todas las columnas de datos de los resultados del informe. ■ **Comprobar** Especifica el operador condicional. ■ **Valor** y **Valor 2** Especifica el valor o los valores que el operador usa para comprobar la condición.

Opción	Descripción
Formato	Le permite configurar los campos apropiados de la plantilla de formato: ■ **Valor de origen** Especifica el origen de los datos que se muestran en la celda con formato. La opción predeterminada es Valor aplicado, que son los datos que ya están en la celda. Sin embargo, eso se puede reemplazar con cualquier otro dato de la misma fila. Para ello, seleccione la columna apropiada. Se muestran todas las columnas de datos de los resultados del informe. ■ **Tipo de origen** Especifica el tipo de valor de origen que se visualizará.

Cuadro de diálogo Editar campos de origen

El cuadro de diálogo **Editar campos de origen** permite modificar la configuración de cada campo de origen incluido en la consulta de recursos.

Ver "Página Edición de informes personalizada: ficha Origen de datos, ficha: Campos " en la página 532.

Tabla D-13 Configuración en el cuadro de diálogo **Editar campos de origen**

Configuración	Descripción
Alias	El alias del campo. Es conveniente especificar un alias de campo para lograr que el SQL sin procesar (que aparece en la ficha **Consulta resuelta**) sea más legible y fácil de comprender.
Seleccionar	Especifica si el campo se incluye o no en los resultados de la consulta. De forma predeterminada, se seleccionan todos los campos.

Configuración	Descripción
Visible	Especifica si el campo se muestra o no en los resultados del informe que el usuario puede ver. De forma predeterminada, todos los campos están visibles. Es posible usar esta opción para ocultar campos determinados al usuario. Por ejemplo, la consulta puede extraer cierta información, como el GUID de un equipo, que no es significativa para el usuario, pero que es útil para otros propósitos. Los datos aún se extraen como parte de los resultados de la consulta, y las políticas de automatización pueden usarlos.
Orden de columnas	Especifica el orden de las columnas en la cuadrícula de resultados del informe. Las columnas se numeran de izquierda a derecha.
Dirección de clasificación	Le permite especificar la dirección de clasificación en la cuadrícula de resultados del informe.
Orden de clasificación	Especifica el orden de clasificación de esta columna en la cuadrícula de resultados del informe. El orden de clasificación se usa con la dirección de clasificación especificada. Cuando se especifican los campos de origen para una consulta de recursos en un informe o filtro, el orden de clasificación se ajusta cuando se cambia la dirección de clasificación. Si cambia el orden de clasificación de un campo según el de otro, el campo que usted cambió se ubica en el orden especificado. Los otros campos se reorganizan como corresponda. Para quitar la clasificación, restablezca el orden de clasificación a N/A. La dirección de clasificación se restablece a Predeterminado y el orden de clasificación de los otros campos se ajusta para completar cualquier intervalo.
Agregar	Le permite especificar cómo agregar los valores en esta columna en la cuadrícula de los resultados del informe.
Orden de grupo	Especifica el orden de clasificación de las filas agregadas.

Configuración	Descripción
Determinación del ámbito	Especifica si el campo debe tener o no un ámbito determinado en los resultados de la consulta. De forma predeterminada, ningún campo tiene un ámbito determinado. Si el campo no tiene un ámbito determinado, la consulta extrae todos los elementos relevantes. Si el campo tiene un ámbito determinado, la consulta extrae solamente los elementos que el usuario que ejecuta la consulta tiene permiso para leer. **Nota:** Los resultados de la consulta que el usuario visualiza como resultados del informe o pertenencia al filtro siempre tienen un ámbito determinado según el rol de usuario. El ámbito se aplica automáticamente cuando se presentan los resultados de la consulta al usuario. Cambiar la configuración aquí no tiene ningún efecto sobre lo que puede ver el usuario.

Cuadro de diálogo Edición de parámetro

El cuadro de diálogo **Edición de parámetro** le permite especificar la configuración de los parámetros de cada parámetro de informe personalizado. En **Parámetro**, puede especificar la configuración general de los parámetros. En **Proveedor de valores**, puede especificar la configuración específica del tipo de proveedor de valores que ha seleccionado.

Ver "Definir parámetros y proveedores de valores para un informe personalizado" en la página 460.

Tabla D-14 Opciones del cuadro de diálogo **Edición de parámetro**

Opción	Descripción
Nombre	Le permite especificar el nombre del parámetro.
Parámetro requerido	Le permite especificar si el parámetro es necesario o no para el informe.
Descripción	Le permite especificar la descripción del parámetro. Esta descripción se usa para identificar el parámetro en la lista desplegable **Agregar parámetro nuevo**.
Tipo	Le permite seleccionar el tipo de parámetro.

Opción	Descripción
Orden de presentación o evaluación	Le permite especificar el orden en que el parámetro se visualiza en la página Informe y el orden en el que el parámetro se evalúa en la consulta del informe. La lista desplegable le permite establecer el valor del orden entre 1 y 19.
Valor predeterminado	Le permite especificar el valor predeterminado para el parámetro. Si el usuario no especifica un valor para el parámetro cuando genera el informe, se usa este valor en la consulta.
Valor de prueba	Le permite especificar el valor de prueba para el parámetro. Este valor se usa cuando se prueba la consulta.
Proveedor de valores	Le permite especificar el proveedor de valores para el parámetro. La configuración del proveedor de valores especifica el tipo de control de la IU que se presenta al usuario. Para cada control de la IU, se puede establecer la configuración relevante, como el ancho del control de la IU, el texto de la etiqueta y el texto de información sobre herramientas. Los tipos disponibles de proveedores de valores dependen del tipo de parámetro que se seleccione.

Apéndice E

Campos que admiten scripts para modificar las reglas de importación y exportación de recursos y las reglas de CMDB

En este Apéndice se incluyen los temas siguientes:

- Campos que admiten scripts para modificar las reglas de importación y exportación de recursos y las reglas de CMDB

Campos que admiten scripts para modificar las reglas de importación y exportación de recursos y las reglas de CMDB

Cuando se utilizan las reglas de importación y exportación de recursos para importar recursos o reglas de CMDB, se asignan o configuran los valores para las columnas del recurso del tipo especificado en la CMDB. Usar una expresión es una de las opciones para configurar valores de columnas. Una expresión le permite escribir algunos scripts de .NET.

La creación de expresiones se documenta en los temas siguientes:

- Ver "Sintaxis de expresiones" en la página 549.
- Ver "Operadores de expresiones" en la página 550.

- Ver "Valores definidos por el usuario" en la página 550.
- Ver "Operadores de cadena" en la página 550.
- Ver "Caracteres comodín" en la página 551.
- Ver "Tipos de agregado" en la página 551.
- Ver "Funciones de expresiones" en la página 551.

Sintaxis de expresiones

Cuando cree una expresión para modificar las reglas de importación y exportación de recursos o las reglas de CMDB, use la propiedad **ColumnName** para consultar columnas. Por ejemplo, si **ColumnName** para una columna es “UnitPrice” y otra es “Quantity”, la expresión es “UnitPrice * Quantity”.

Cuando cree una expresión para un filtro, incluya las cadenas entre comillas simples. Por ejemplo:

```
'LastName = 'Jones'.'
```

Si usa los caracteres especiales siguientes en un columnname, se deben escapar:

\n (newline)	\	*	[	"
\t (tab)	/	%	]	#
\r (carriage return)	=	&	'	-
~	>	|	+	)
(	<	^		

Si un nombre de columna contiene uno de los caracteres en la tabla precedente, el nombre debe incluirse entre corchetes. Por ejemplo, para usar una columna denominada “Column#” en una expresión, se escribiría:

```
[Column#]”. Ejemplo: Total * [Column#]
```

Si se incorporará una fecha, deberá usar el formato mes/día/año. Los formatos día/mes/año o año/mes/día no son válidos.

Como los corchetes son caracteres especiales, es necesario usar una barra diagonal ("\") para escapar el corchete, si es parte de un nombre de columna. Por ejemplo, una columna denominada “Column[]” sería escrita:

```
“Total * [Column[\]]”
```

Solamente el segundo corchete se debe escapar.

Ver "Campos que admiten scripts para modificar las reglas de importación y exportación de recursos y las reglas de CMDB" en la página 548.

Operadores de expresiones

La concatenación se admite dentro de expresiones usando los operadores booleanos AND, OR y NOT. Es posible usar paréntesis para agrupar cláusulas y establecer órdenes de precedencia. El operador AND tiene precedencia sobre otros operadores. Ejemplo: (LastName = 'Smith' OR LastName = 'Jones') AND FirstName = 'John'

Cuando se crean expresiones de comparación, los operadores siguientes están permitidos:

<	>	<=	>=	<>
=	IN	LIKE		

Cuando se crean expresiones aritméticas de comparación, los operadores siguientes están permitidos:

+ (adición)	- (sustracción)	* (multiplicación)	/ (división)	% (módulo)

Ver "Campos que admiten scripts para modificar las reglas de importación y exportación de recursos y las reglas de CMDB" en la página 548.

Valores definidos por el usuario

Los valores definidos por el usuario se pueden usar dentro de las expresiones que se compararán con valores de la columna. Los valores de cadena deben ser incluidos entre comillas. Los valores de fecha deben ser incluidos entre símbolos de almohadillas (#). Los decimales y la notación científica se permiten para los valores numéricos. Ejemplos: "FirstName = 'John'"; "Price <= 50.00"; "Birthdate < #1/31/ 82#".

Para las columnas que contienen valores de enumeración, se convierte el valor a un tipo de datos de número entero. Ejemplo: “EnumColumn = 5"

Ver "Campos que admiten scripts para modificar las reglas de importación y exportación de recursos y las reglas de CMDB" en la página 548.

Operadores de cadena

Para concatenar una cadena en una expresión, use el carácter +.

Ver "Campos que admiten scripts para modificar las reglas de importación y exportación de recursos y las reglas de CMDB" en la página 548.

Caracteres comodín

Ambos * y % se pueden usar en expresiones indistintamente para los comodines en una comparación LIKE. Si la cadena en una cláusula de LIKE contiene un * o %, esos caracteres se deben escapar en corchetes ([]). Si hay un corchete en la cláusula, los caracteres de corchete se deben escapar en corchetes. Ejemplo: [[] o []]. Un comodín está permitido al principio y al final de un patrón o al final de un patrón o al principio de un patrón. Ejemplos: "ItemName LIKE '*product*'"; "ItemName LIKE '*product'"; "ItemName LIKE 'product*'".

Los comodines no están permitidos en el medio de una cadena. Por ejemplo, 'te*xt' no está permitido.

Ver "Campos que admiten scripts para modificar las reglas de importación y exportación de recursos y las reglas de CMDB" en la página 548.

Tipos de agregado

Es posible usar los tipos de agregado siguientes en las expresiones:

Sum (Sum)	Avg (Average)	Min (Minimum)	Max (Maximum)
Count (Count)	StDev (Statistical standard deviation)	Var (Statistical variance)	

Cree una expresión de agregado usando una de las funciones anteriormente detalladas. Por ejemplo, use Sum(Price) para crear un resumen de cifras en una columna denominada “Price”. No existe la función Agrupar por; por lo tanto, todas las filas muestran el mismo valor en la columna. Si una tabla no tiene ninguna fila, las funciones de agregado devuelven una referencia nula.

Ver "Campos que admiten scripts para modificar las reglas de importación y exportación de recursos y las reglas de CMDB" en la página 548.

Ver "Función Convert" en la página 552.

Funciones de expresiones

Es posible elegir las siguientes funciones de expresiones:

- Convert
  Ver "Función Convert" en la página 552.
- Len

Ver "Función Len" en la página 552.

- IsNull
  Ver "Función IsNull" en la página 553.
- IIF
  Ver "Función IIF" en la página 553.
- Trim
  Ver "Función Trim" en la página 554.
- Substring
  Ver "Función Substring" en la página 554.

Ver "Campos que admiten scripts para modificar las reglas de importación y exportación de recursos y las reglas de CMDB" en la página 548.

Función Convert

Convierte una expresión a un tipo especificado de tipo de .NET Framework.

Sintaxis: `Convert(expression, type)`

Tabla E-1 Argumentos de la función Convert

Argumento	Descripción
expression	Especifica la expresión para convertir.
type	Especifica el tipo de .NET Framework al cual se convierte el valor.

Ejemplo: `myDataColumn.Expression="Convert(total, 'System.Int32')"`

Todas las conversiones son válidas, con las excepciones siguientes:

- Los operadores booleanos se pueden convertir en y de Byte, SByte, Int16, Int32, Int64, UInt16, UInt32, UInt64, String y a sí mismos solamente.
- El carácter se puede convertir en y de Int32, UInt32, String y a sí mismo solamente.
- La fecha y hora se puede convertir en y de String y a sí mismo solamente.
- El marco temporal se puede convertir en y de String y a sí mismo solamente.

Ver "Funciones de expresiones" en la página 551.

Función Len

Obtiene la longitud de una cadena.

Sintaxis: `Len(expression)`

Tabla E-2 Argumentos de la función Len

Argumento	Descripción
expression	Especifica la cadena que se evaluará.

Ejemplo: `myDataColumn.Expression="Len(ItemName)"`

Ver "Funciones de expresiones" en la página 551.

Función IsNull

Comprueba una expresión y devuelve la expresión comprobada o un valor de reemplazo.

Sintaxis: `IsNull(expression, replacementvalue)`

Tabla E-3 Argumentos de la función IsNull

Argumento	Descripción
expression	Define la expresión para comprobar.
replacementvalue	Define el valor para devolver si la expresión es una referencia nula (nada).

Ejemplo: `myDataColumn.Expression="IsNull(price, -1)"`

Ver "Funciones de expresiones" en la página 551.

Función IIF

Obtiene uno de dos valores según el resultado de una expresión lógica.

Sintaxis: `IIF(expression, truepart, falsepart)`

Tabla E-4 Argumentos de la función IIF

Argumento	Descripción
expression	Define la expresión para evaluar.
truepart	Define el valor para devolver si la expresión es verdadera.
falsepart	Define el valor para devolver si la expresión es falsa.

Ejemplo: `myDataColumn.Expression = "IIF(total>1000, 'expensive', 'dear')`

Ver "Funciones de expresiones" en la página 551.

Función Trim

Elimina todos los caracteres iniciales y finales en blanco, por ejemplo, \r,\n,\t, ' '

Sintaxis: `Trim(expression)`

Tabla E-5 Argumentos de la función Trim

Argumento	Descripción
expression	Define la expresión para recortar.

Ver "Funciones de expresiones" en la página 551.

Función Substring

Obtiene una subcadena de una longitud especificada, que se inicia en un punto especificado en la cadena.

Sintaxis: `Substring(expression, start, length)`

Tabla E-6 Argumentos de la función Substring

Argumento	Descripción
expression	Define la cadena de origen para la subcadena.
start	Especifica un número entero que define dónde la subcadena comienza.
length	Especifica el número entero que define la longitud de la subcadena.

Ejemplo: `myDataColumn.Expression = "Substring(phone, 7, 8)"`

Es posible restablecer la propiedad Expression asignándole un valor nulo o una cadena vacía. Si un valor predeterminado se configura en la columna Expression, a todas las filas previamente completadas se asigna el valor predeterminado una vez que la propiedad Expression se restablece.

Ver "Funciones de expresiones" en la página 551.

Apéndice F

Avisos legales de otros fabricantes de Symantec™ Management Platform 7.5

En este Apéndice se incluyen los temas siguientes:

- Avisos legales de otros fabricantes
- 7-Zip
- Apache HTTP Server
- Apache Xerces C++
- Boost
- Bouncy Castle
- Curl
- glibc
- Libatomics_Ops
- LibXML2
- Makeself
- Microsoft Anti-Cross Site Scripting Library
- OpenPegasus
- OpenSSL 0.9.8u
- OpenSSL 0.9.8y

- OpenSSL 1.0.1e
- plists-cs
- SQLite
- Windows Template Library 'WTL' v8.0
- Zlib

Avisos legales de otros fabricantes

Este producto de Symantec puede contener software de otros fabricantes que Symantec debe atribuir al otro fabricante (“Programas de otros fabricantes”). Algunos Programas de otros fabricantes están disponibles con licencias de código abierto o de software gratuito. El Acuerdo de licencia que acompaña el Software no altera ningún derecho ni obligación que pueda tener conforme a las licencias de código abierto o de software gratuito. En este apéndice, se incluyen avisos de propietarios de Programas de otros fabricantes y las licencias de tales programas, según corresponda.

7-Zip

7-Zip v9.20 [2010-11-18] for Windows

Copyright (c) 1999-2010 Igor Pavlov

All copyrights to original unRAR code are owned by Alexander Roshal

MIT License

This code is licensed under the license terms below, granted by the copyright holder listed above. The term "copyright holder" in the license below means the copyright holder listed above.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES

OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Apache HTTP Server

Apache HTTP Server v2.2.22

Portions of this program contain components from the Apache Software Foundation. These components are made available under the Apache License 2.0, a copy of which is provided herein.

Apache License, Version 2.0

January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License.

Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License.

Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or

contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution.

You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

- You must give any other recipients of the Work or Derivative Works a copy of this License; and
- You must cause any modified files to carry prominent notices stating that You changed the files; and
- You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
- If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions.

Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks.

This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty.

Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability.

In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability.

While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

Apache Xerces C++

Apache Xerces C++ v3.0

Copyright © 2012 The Apache Software Foundation, Licensed under the Apache License, Version 2.0.

Apache and the Apache feather logo are trademarks of The Apache Software Foundation.

Apache License, Version 2.0

January 2004

http://www.apache.org/licenses/

TÉRMINOS Y CONDICIONES PARA EL USO, REPRODUCCIÓN Y DISTRIBUCIÓN

1. Definiciones.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the

copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License.

Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License.

Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution.

You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

- You must give any other recipients of the Work or Derivative Works a copy of this License; and
- You must cause any modified files to carry prominent notices stating that You changed the files; and
- You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of

the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

- If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. Los contenidos del archivo de AVISO son para propósitos informativos solamente y no modifican la Licencia. Es posible agregar sus propios avisos de atribución dentro de los trabajos derivados que se distribuyen, junto con o como adición al texto de AVISO del trabajo, a condición de que tales avisos adicionales de atribución no se puedan interpretar como modificación de la Licencia.

Es posible agregar su propia declaración de copyright a sus modificaciones y puede proporcionar términos y condiciones de licencia adicionales o diferentes para el uso, la reproducción o la distribución de sus modificaciones o para tales trabajos derivados en conjunto, con tal que su uso, reproducción y distribución del trabajo cumpla de otra manera con las condiciones indicadas en esta Licencia.

5. Submission of Contributions.

Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Marcas comerciales.

Esta Licencia no concede el permiso para usar los nombres comerciales, las marcas comerciales, las marcas de servicio o los nombres de producto del emisor de la licencia, excepto en caso de necesidad para el uso razonable y habitual en la descripción del origen del trabajo y la reproducción del contenido del archivo de AVISO.

7. Renuncia de responsabilidad de la garantía.

A menos que fuera requerido por la ley aplicable o estuviera acordado por escrito, el emisor de la licencia proporciona el trabajo (y cada contribuidor proporciona sus contribuciones) "TAL CUAL", SIN GARANTÍAS NI CONDICIONES DE NINGUNA CLASE, expresas o implicadas, incluyendo, sin limitaciones, cualquier garantía o condición de TÍTULO, NO VIOLACIÓN DE DERECHOS, COMERCIABILIDAD o APTITUD PARA UN PROPÓSITO DETERMINADO. You are solely responsible

for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability.

In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability.

While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

FINAL DE LOS TÉRMINOS Y CONDICIONES

Boost

Boost v1.42.0

Copyright Joe Coder 2004 - 2006.

Boost Software License - Version 1.0 - August 17th, 2003

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Bouncy Castle

Bouncy Castle v1.5

The Legion Of The Bouncy Castle

Copyright (c) 2000 - 2010 The Legion Of The Bouncy Castle (http://www.bouncycastle.org)

MIT License

This code is licensed under the license terms below, granted by the copyright holder listed above. The term copyright holder” in the license below means the copyright holder listed above.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Curl

Curl v7.24.0

Copyright (c) 1996 - 2011, Daniel Stenberg, <daniel@haxx.se>.All rights reserved

COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1996 - 2011, Daniel Stenberg, <daniel@haxx.se>.

All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

glibc

glibc i686 rpm v2.12-1.7

Free Software Foundation, a wide variety of years

Copyright (C) 1991 Regents of the University of California.

Portions Copyright (C) 1993 by Digital Equipment Corporation.

Copyright (C) 1984, Sun Microsystems, Inc.

Copyright (C) 1991,1990,1989 Carnegie Mellon University

Copyright (c) 2000, Intel Corporation copyright (C) by Craig Metz, no year specified

The code may be accessed at: http://rhn.redhat.com

GNU Lesser General Public License

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that

the original author's reputation will not be affected by problems that might be introduced by others.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the

Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he

or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO

MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and an idea of what it does.> Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

signature of Ty Coon, 1 April 1990 Ty Coon, President of Vice

Libatomics_Ops

Hewlett-Packard Development Company, L.P., Xerox Corporation, Silicon Graphics & Hewlett-Packard Company.

Copyright (c) 2003-2004 Hewlett-Packard Development Company, L.P.

Copyright (c) 1991-1994 by Xerox Corporation. All rights reserved.

Copyright (c) 1996-1999 by Silicon Graphics. All rights reserved.

Copyright (c) 1999-2003 by Hewlett-Packard Company. All rights reserved.

Our intent is to make it easy to use libatomic_ops, in both free and proprietary software. Hence most code that we expect to be linked into a client application is covered by an MIT-style license.

A few library routines are covered by the GNU General Public License. These are put into a separate library, libatomic_ops_gpl.a .

The low-level part of the library is mostly covered by the following license:

Copyright (c) ...

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

A few files in the sysdeps directory were inherited in part from the Boehm-Demers-Weiser conservative garbage collector, and are covered by its license, which is similar in spirit:

Copyright (c) ...

THIS MATERIAL IS PROVIDED AS IS, WITH ABSOLUTELY NO WARRANTY EXPRESSED OR IMPLIED. ANY USE IS AT YOUR OWN RISK.

Permission is hereby granted to use or copy this program for any purpose, provided the above notices are retained on all copies. Permission to modify the code and to distribute modified code is granted, provided the above notices are retained, and a notice that the code was modified is included with the above copyright notice.

A few files are covered by the GNU General Public License. (See file "COPYING".) This applies only to test code, sample applications, and the libatomic_ops_gpl portion of the library. Thus libatomic_ops_gpl should generally not be linked into proprietary code. (This distinction was motivated by patent considerations.)

It is possible that the license of the GPL pieces may be changed for future versions to make them more consistent with the rest of the package. If you submit patches, and have strong preferences about licensing, please express them.

LibXML2

Copyright (C) 1998-2003 Daniel Veillard. All Rights Reserved.

MIT License

This code is licensed under the license terms below, granted by the copyright holder listed above. The term copyright holder” in the license below means the copyright holder listed above.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Makeself

Makeself v2.1.5

(C) 1998-2008 by Stéphane Peter <megastep@megastep.org>

The source code for this component may be obtained from Symantec Corporation upon request.

The GNU General Public License (GPL)

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary

way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include

anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the

sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

One line to give the program's name and a brief idea of what it does. Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'. This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision' (which makes passes at compilers) written by James Hacker.

signature of Ty Coon, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

Microsoft Anti-Cross Site Scripting Library

Microsoft Anti-Cross Site Scripting Library v4.2.1

Copyright (c) 2010 Microsoft Corporation

Microsoft Public License (Ms-PL)

This license governs use of the accompanying software. If you use the software, you accept this license. If you do not accept the license, do not use the software.

1. Definitions

The terms "reproduce," "reproduction," "derivative works," and "distribution" have the same meaning here as under U.S. copyright law. A "contribution" is the original software, or any additions or changes to the software. A "contributor" is any person that distributes its contribution under this license. "Licensed patents" are a contributor's patent claims that read directly on its contribution.

2. Grant of Rights

(A) Copyright Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce its contribution, prepare derivative works of its contribution, and distribute its contribution or any derivative works that you create.

(B) Patent Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide,

royalty-free license under its licensed patents to make, have made, use, sell, offer for sale, import, and/or otherwise dispose of its contribution in the software or derivative works of the contribution in the software.

3. Conditions and Limitations

(A) No Trademark License- This license does not grant you rights to use any contributors' name, logo, or trademarks.

(B) If you bring a patent claim against any contributor over patents that you claim are infringed by the software, your patent license from such contributor to the software ends automatically.

(C) If you distribute any portion of the software, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.

(D) If you distribute any portion of the software in source code form, you may do so only under this license by including a complete copy of this license with your distribution. If you distribute any portion of the software in compiled or object code form, you may only do so under a license that complies with this license.

(E) The software is licensed "as-is." You bear the risk of using it. The contributors give no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this license cannot change. To the extent permitted under your local laws, the contributors exclude the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

OpenPegasus

OpenPegasus v2.7.0

Copyright (c) 2000, 2001, 2002 BMC Software; Hewlett-Packard Development

// Company, L.P.; IBM Corp.; The Open Group; Tivoli Systems.

// Copyright (c) 2003 BMC Software; Hewlett-Packard Development Company, L.P.;

// IBM Corp.; EMC Corporation, The Open Group.

// Copyright (c) 2004 BMC Software; Hewlett-Packard Development Company, L.P.;

// IBM Corp.; EMC Corporation; VERITAS Software Corporation; The Open Group.

// Copyright (c) 2005 Hewlett-Packard Development Company, L.P.; IBM Corp.;

// EMC Corporation; VERITAS Software Corporation; The Open Group.

// Copyright (c) 2006 Hewlett-Packard Development Company, L.P.; IBM Corp.;

// EMC Corporation; Symantec Corporation; The Open Group.

MIT License

This code is licensed under the license terms below, granted by the copyright holder listed above. The term copyright holder" in the license below means the copyright holder listed above.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

OpenSSL 0.9.8u

Eric Young & Tim Hudson Copyright (c) 1998-2011.

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

'This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)'

License

This is a copy of the current LICENSE file inside the CVS repository.

LICENSE ISSUES

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

/*==========

*Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved.

* Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* 3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

* "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

* 5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

* 6. Redistributions of any form whatsoever must retain the following acknowledgment:

* "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

* This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

* All rights reserved.

* This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

* The implementation was written so as to conform with Netscape SSL.

* This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

* Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

* If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.

* This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

* Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* 1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

* 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* 3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

* "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

* The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

* 4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

* "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR

CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

* The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

OpenSSL 0.9.8y

Copyright (c) 1998-2011 The OpenSSL Project

Copyright (c) 1995-1998 Eric A. Young, Tim J. Hudson

All rights reserved.

'This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)'

This product includes software written by Tim Hudson (tjh@cryptsoft.com)

License

This is a copy of the current LICENSE file inside the CVS repository.

LICENSE ISSUES

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

/*==

*Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved.

* Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* 3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

* "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

* 5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

* 6. Redistributions of any form whatsoever must retain the following acknowledgment:

* "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

* This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

* All rights reserved.

* This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

* The implementation was written so as to conform with Netscape SSL.

* This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

* Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

* If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.

* This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

* Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* 1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

* 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* 3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

* "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

* The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

* 4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

* "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)

ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

* The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

OpenSSL 1.0.1e

Copyright (c) 1998-2011 The OpenSSL Project

Copyright (c) 1995-1998 Eric A. Young

All rights reserved.

'This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)'

This product includes software written by Tim Hudson (tjh@cryptsoft.com)

License

This is a copy of the current LICENSE file inside the CVS repository.

LICENSE ISSUES

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

/*==========

*Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved.

* Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* 3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

* "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

* 5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

* 6. Redistributions of any form whatsoever must retain the following acknowledgment:

* "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

* This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

* All rights reserved.

* This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

* The implementation was written so as to conform with Netscape SSL.

* This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

* Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

* If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.

* This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

* Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* 1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

* 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* 3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

* "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

* The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

* 4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

* "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

* The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

plists-cs

plists-cs v1.3.zip - v1.30.0

Copyright (c) 2011 Chad Burggraf

MIT License

This code is licensed under the license terms below, granted by the copyright holder listed above. The term copyright holder” in the license below means the copyright holder listed above.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

SQLite

SQLite v3.3.17

This component is in the public domain.

This software is placed in the public domain. It is provided “AS IS” without warranty or support of any kind.

Windows Template Library 'WTL' v8.0

Copyright © 2007 Microsoft Corporation. All rights reserved.

Microsoft Permissive License

This license governs use of the accompanying software. If you use the software, you accept this license. If you do not accept the license, do not use the software.

1. Definitions

The terms “reproduce,” “reproduction” and “distribution” have the same meaning here as under U.S. copyright law.

“You” means the licensee of the software.

“Licensed patents” means any Microsoft patent claims which read directly on the software as distributed by Microsoft under this license.

2. Grant of Rights

(A) Copyright Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, Microsoft grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce the software, prepare derivative works of the software and distribute the software or any derivative works that you create.

(B) Patent Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, Microsoft grants you a non-exclusive, worldwide, royalty-free patent license under licensed patents to make, have made, use, practice, sell, and offer for sale, and/or otherwise dispose of the software or derivative works of the software.

3. Conditions and Limitations

(A) No Trademark License- This license does not grant you any rights to use Microsoft’s name, logo, or trademarks.

(B) Platform Limitation- The licenses granted in sections 2(A) & 2(B) extend only to the software or derivative works that you create that run on a Microsoft Windows operating system product.

(C) If you begin patent litigation against Microsoft over patents that you think may apply to the software (including a cross-claim or counterclaim in a lawsuit), your license to the software ends automatically.

(D) If you distribute copies of the software or derivative works, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.

(E) If you distribute the software or derivative works in source code form you may do so only under this license (i.e., you must include a complete copy of this license with your distribution), and if you distribute the software or derivative works in compiled or object code form you may only do so under a license that complies with this license.

(F) The software is licensed “as-is.” You bear the risk of using it. Microsoft gives no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this license cannot change. To the extent permitted under your local laws, Microsoft excludes the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

Zlib

Copyright (C) 1995-2010 Jean-loup Gailly and Mark Adler

zlib/libpng License

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

Índice

A

Actualizaciones de software
  instalación 187
  programar descarga 187
Actualizar datos de resumen
  informes de jerarquía 170
Administración de parches
  programar 187
Administración de recurso. *Ver* Administrador de recursos
Administración de tareas
  acerca de 407
Administración habilitada para la nube
  acerca de 284
  actividades necesarias de antemano 287
  configurar la política de configuración de administración habilitada para la nube 320
  conmutadores de línea de comandos AeXNSAgent.exe 523
  entorno mixto 517
  gateway de Internet 307
  herramientas de la línea de comandos 516
  informes 338
  paquete de instalación del agente, generando 522
  paquete de instalación del agente, parámetros 522
  preparar el entorno 287
  preparar los servidores de sitio 287
  revocar el certificado 332
  servidores de paquetes 518
  servidores de sitio 518
  Task Servers 518
Administrador de recursos
  abrir desde resultados del informe 444
  acceso 434
  acerca de 433
  adición de un recurso 436
  tareas 437
  visualización de datos 435
  visualización de datos del evento 436
Administrador de roles de seguridad
  acceso 113
  acerca de 113
AeXGenClientCert.exe
  descripción general 516
  parámetros de línea de comandos 328
AeXGenSiteServerCert.exe
  descripción general 516
  parámetros de línea de comandos 296
AeXNSAgent.exe
  conmutadores de línea de comandos 523
AeXRevokeCertificate.exe
  descripción general 516
  parámetros de línea de comandos 332
Agente. *Ver* Symantec Management Agent
Agente de la solución
  política de actualización 389
  política de desinstalación 389
  política de instalación 389
agente de tareas del cliente
  configuración 430
Agente habilitado para la nube
  cómo instalar un certificado de cliente temporal 331
  conmutadores de línea de comandos 523
  eliminar el certificado de cliente 331
  instalación en un equipo desconectado 323
  selección del gateway de Internet, forzar 335
  solucionar problemas 327
Agregado
  tipos 551
Ajuste automático
  configuración de agente y tareas 184
Ámbito del recurso
  acerca de 348
  cómo hacerlo 348
  destinos 348
  filtros 348
  vistas organizativas 348
Archivado
  datos de tarea 429

Archivar
datos de la versión de la tarea 429
Archivo CSV
importación de equipos 246
archivo CSV
guardar resultados de informe 446
archivo HTML
guardar resultados de informe 446
archivo XML
exportación de elementos de la consola 63
guardar elementos de la consola 63
guardar menú de consola 53
guardar resultados de informe 446
importación de submenú de la consola 53
importación del menú de consola 53
restauración de elementos de la consola 63
Archivos MIB
importar 233
ARP 216
Arrastrar y soltar
aplicar la política 378
ejecución de tareas y trabajos 420
Asistente de Network Discovery 212
Ayuda
acceder a 50
contextual 31
Ayuda contextual 31

B

Base de datos de la administración de configuración. *Ver* CMDB
Buscar un equipo 39
Buscar un software 42
Búsqueda de equipos
ejecución 39
guardar como filtro 39
Búsqueda de software
configuración de límites 47
guardado 42
realización 42
Búsqueda de un equipo 45
configuración de límites 47
configuración del campo de búsqueda 47
Búsqueda de un software 45
configuración del campo de búsqueda 47
Búsquedas guardadas
administrar 42

C

Cadena
operadores 550
Campos que admiten scripts
Substring 548
Cantidad máxima de subprocesos
Network Discovery 210
Carpeta
cómo tomar propiedad 115
configuración de los permisos de herencia 104
configurar permisos 103
Certificado
aplicar al equipo administrado 292
exportar desde Notification Server 292
Certificado de CEM
revocar 332
Certificado de cliente
generación con AeXGenClientCert.exe 328
Certificado de Notification Server
aplicar al equipo administrado 292
exportar de Notification Server 292
Certificado de servidor
aplicación al servidor de sitio 296
generación con AeXGenSiteServerCert.exe 296
Clase de datos
virtual 486
visualización de datos de inventario para 435
visualización de datos del evento para 436
Clase de datos virtual
crear 486
Clasificaciones de dispositivos SNMP 210
Clave de búsqueda de recursos
creación 481
CMDB
acerca de 76
Autenticación de Windows 76
autenticación SQL 76
configuración 76
credenciales de acceso a la base de datos 76
credenciales públicas del informe 76
depuración de datos antiguos 80
historial de datos de recursos 82
nombre de la base de datos 76
nombre del servidor de la base de datos 76
tiempo de espera de comando 76
Cómo crear y ejecutar tareas de detección de redes
cómo habilitar Supervisores de Symantec 226
Comodín
caracteres 551

Comunicación de agente de una versión anterior
acerca de 272
activación 272
desactivación 272
deshabilitar 69
estados predeterminados 272
habilitar 69
Confianza de agente
aceptar 243
acerca de 237
bloquear 243
establecimiento 237
política de registro 243
revocar 251
Configuración
configuración por primera vez 177
configurar con el configurador de NS 75
configuración
agente de tareas del cliente 430
Task Server 430
Configuración de agente y tareas
ajuste automático 184
optimización 184
Configuración de HTTPS
en el equipo administrado 292
configuración de ICMP
tarea de Detección de red 214
Configuración de instalación
Symantec Management Agent para UNIX, Linux y Mac 259
configuración de protocolo
tarea de Detección de red 214
configuración de SNMP
tarea de Detección de red 214
Configuración del agente
ajuste automático 181
optimización 181
Configuración del agente de CEM
configurar 311
Configuración por primera vez
portal 177
Configurador de NS
acerca de 75
consola. *Ver* Symantec Management Console
Consulta de informe
acerca de 457
adición de expresiones de filtro en una consulta 535
campos de origen
adición a consulta de recursos 532
edición 544
campos de origen de consulta SQL 533
consulta de recurso 457
Consulta SQL 459
conversión de una consulta de recurso en una consulta SQL 457
determinación del ámbito de la instantánea de datos 535
escribir una consulta SQL 533
generación de una consulta de recursos 529
parámetro de consulta
acerca de 534
parámetro de informes
adición 460
adición de tipo avanzado 460
configuración 546
creación 460
modificación 460
parámetro de informes, definición 460
visualización de consulta resuelta 537
visualización de resultados de consulta 538
Consulta de recurso
adición de expresiones de filtro en una consulta 535
definición para filtro 358
parámetro de consulta
acerca de 534
parámetro de informes
adición 460
creación 460
modificación 460
parámetro de informes, definición 460
visualización de resultados de consulta 538
Consulta de recursos
campos de origen
adición 532
edición 544
generación con Generación de consultas 529
origen de datos para política de automatización 401
parámetro de informes
adición de tipo avanzado 460
visualización de consulta resuelta 537
Consulta del filtro
adición de expresiones de filtro en una consulta 535
campos de origen de consulta SQL 533

conversión de una consulta de recurso en una consulta SQL 457
escribir una consulta SQL 533
generación de una consulta de recursos 529
parámetro de consulta
acerca de 534
visualización de resultados de consulta 538
consulta del filtro
acerca de 457
visualización de consulta resuelta 537
Consulta del recurso
parámetro de informes
configuración 546
Consulta SQL
definición para filtro 360
determinación del ámbito de instantáneas de informe 535
escritura 533
inserción de campos de origen 533
instantánea de datos 535
origen de datos para política de automatización 401
parámetro de consulta
acerca de 534
parámetro de informes
adición 460
adición de tipo avanzado 460
configuración 546
creación 460
modificación 460
parámetro de informes, definición 460
visualización de consulta resuelta 537
visualización de resultados de consulta 538
Credencial
creación 115
edición 115
Credential Manager
acerca de 115
Criterios de búsqueda personalizados
crear 39, 42
Cuenta de usuario
asignación a roles de seguridad 102
cómo desbloquear las credenciales 113
configuración 94
configuración de la complejidad de la contraseña 110
configuración de permisos de herencia en carpetas 104
configuración del bloqueo de la contraseña 110
creación 94
detalles generales de la cuenta 98

D

Data Connector
acerca de 474
capacidades 476
cómo funciona 475
usos 476
Datos
preproceso 479
Datos de eventos de recursos
depurar 80
Datos de la CMDB
edición 484
Datos de la versión de la tarea
limpiar 429
Datos de recurso
visualización 435
Datos de tarea
limpieza 429
Datos de versión anterior del informe
depurar 80
Datos del equipo
depurar 80
Datos del evento
visualización 436
DefaultAppPool
configuración 310
Definición de origen de datos
creación 479
Definidos por el usuario
valores 550
Depurar ahora 80
descubrimiento de recursos
acerca de 190
detectar equipos con 192
Destino
acerca de 366
dependencia en filtro 365
destino con nombre, abrir 383
destino con nombre, acerca de 366, 379
destino con nombre, guardar 384
destino con nombre, seleccionar 386
destino generado automáticamente, acerca de 366, 379
destino generado automáticamente, guardar 382
especificación de política 379
exclusión de elementos 385

grupos de destinos 386
inclusión de elementos 385
modificación 381
programación de actualización 367
reglas de filtro 385
seleccionar equipos 382
seleccionar recursos 382
seleccionar usuarios 382
Destino de recursos. *Ver* Destino
detección
dispositivos de red 208
Importación de Active Directory 190
Network Discovery 190
Pertenencia al dominio 190
recursos 190
Detección de dispositivos 208
Detección de dispositivos de red 209
detección de recursos
importación de Active Directory 190
Network Discovery 190
Pertenencia al dominio 190
Detección de redes
delegación de tareas de detección 231
delegar tareas 221, 224, 229, 231–232
proceso para delegar tareas 221
Detectar equipos 179
Directiva
dependencia en filtro 365
directiva
configuración del agente de destino 278
Destino 366
Dispositivos de red
cómo permitir a otros usuarios detectar 221
delegación de tareas de detección 221, 224, 226, 229, 232
Dispositivos SNMP
clasificación 220
Documentación 31
acceder a 50

E

Editor de programaciones
abrir 122
uso 123
Ejecución de tareas
jerarquía 413
Elemento
cómo tomar propiedad 115
configurar permisos 103
elemento de menú
adición al menú de la consola 53
exportar 53
importar 53
Elemento web
acerca del uso de páginas del portal 59
elemento web
adición a la página del portal 59
configuración de la altura fija 61
configuración del tamaño predeterminado 61
creación 61
creación a partir de informe 448
modificación 61
mostrar resultados del informe 61
mostrar URL 61
Eliminación
datos de tarea 429
Eliminar
datos de la versión de la tarea 429
Entrada de la tarea
recepción 426
Entradas del registro del agente
depurar 80
Equipo
acerca de la detección 191
buscar 39, 45
cómo desinstalar manualmente Symantec Management Agent 274
cómo instalar en modo push Symantec Management Agent para UNIX, Linux y Mac 260
cómo instalar manualmente Symantec Management Agent 240, 255
cómo instalar Symantec Management Agent 238
cómo instalar Symantec Management Agent en modo push 246
cómo seleccionar para la instalación de Symantec Management Agent 246
configuración de las políticas de Symantec Management Agent 276
configuración de una ventana de mantenimiento 280
configuración del agente de destino 278
configuración global de agente 277
detectar con la Detección de recursos 192
detectar con la importación de Active Directory 199
instalación programada de Symantec Management Agent 249

instalación remota de Symantec Management Agent 247
instalación remota de Symantec Management Agent para UNIX, Linux y Mac 264
intervalos de actualización de datos de Symantec Management Agent 510
métodos de detección 191
Política de actualización de Symantec Management Agent 268
Política de desinstalación de Symantec Management Agent 268
requisitos previos para instalar Symantec Management Agent 242
Symantec Management Agent 236
ventana de mantenimiento 280
Equipos
detectar 179
Estado de registro del agente
informe 251
Evaluación
licencia 30
Exportación de datos 477
expresión
operadores 550
sintaxis 549

F

Filtro
actualizar pertenencia 363
consulta de recurso 358
creación 355
dependencias 365
ejecución de acciones en recursos 364
exclusiones 361
inclusiones 361
menú contextual para los miembros 364
modificación 356
selección del tipo de consulta 357
filtro
acerca de 353
consulta 457
Ver también consulta del filtro
Consulta SQL 360
creación de filtro estático a partir de resultados del informe 447
proceso para crear 354
programación de las actualizaciones de pertenencia 367
Filtro de recurso. *Ver* filtro
filtro estático
creación a partir de resultados del informe 447
Función
Convert 552
expresión 551
IIF 553
IsNull 553
Len 552
Substring 554
Trim 554

G

Gateway de Internet
administración 520
anular el registro del servicio de gateway de Internet, script 520
aplicar el certificado de Notification Server, script 520
aplicar la lista de revocación del certificado, script 520
archivos de configuración 307
archivos de registro 307
certificado de servidor de regeneración, script 520
cómo forzar la selección en el agente habilitado para la nube 335
configuración 317
configurar 307
configurar el equipo host 313
descargar paquete de instalación 315
descripción general 307
detener el servicio de gateway de Internet, script 520
ejecutar paquete de instalación 315
equilibrio de carga 521
hacer copia de seguridad 336
iniciar el servicio de gateway de Internet, script 520
preparación 313
proceso de instalación 307
puerto 317
registrar el servicio de gateway de Internet, script 520
restauración completa 336
restauración parcial 336
Generación de consultas
uso para consulta de filtro 358
Grupo organizativo
acerca de 344

adición de un recurso a 436
agregar equipos 344
agregar recursos 344
agregar usuarios 344
asignación de roles de seguridad 346
configuración de permisos de administración de recursos 346
configuración de permisos de seguridad personalizados 346
configuración de permisos de Task Server 346
configuración de permisos del sistema 346
editar un grupo 344
uso en la seguridad de recursos 340
grupo organizativo
administración 345
ejecución de acciones en miembros 345
programación de actualización 367
visualización de recursos 345

H

Herramienta de la línea de comandos
AeXGenClientCert.exe 516
AeXGenSiteServerCert.exe 516
AeXRevokeCertificate.exe 516
Historial de datos de recursos
almacenamiento en la CMDB 82

I

Identidad de la aplicación
Notification Server 69
Importación de Active Directory
acerca de 197
asociaciones de recursos, importar 198
detectar equipos 199
ejecutar importaciones de recursos manualmente 206
importaciones completas 204
importaciones de actualización 204
informes 197
proceso para usar 199
programación de importaciones de recursos 204
Programación de sincronización del directorio 205
registro de errores 197
regla de importación de recursos 201
tipos de recursos admitidos 201
importación de Active Directory
detección de recursos 190
Importación de datos 477
Información de estado de tarea
jerarquía 413
Informe
acerca de 439
creación. *Ver* Informe personalizado
especificación de parámetros de usuario 441
estado de la instalación de Symantec Management Agent 250
examen de niveles inferiores de resultados 444
extracción de resultados 441
impresión de resultados 444
informes de jerarquía 169
modificación. *Ver* Informe personalizado
origen de datos para política de automatización 401
personalizar. *Ver* Informe personalizado
proceso para usar 440
realización de acciones en elementos de resultados 444
selección de instantánea 441
vista de cuadrícula, seleccionar 443
vista de gráfico, seleccionar 443
vista de resultados 443
informe
guardar como elemento web 448
guardar instantánea 448
guardar resultados como filtro estático 447
guardar resultados en un archivo 446
Informe de equipo. *Ver* Informe personalizado
Informe de SQL. *Ver* Informe personalizado
Informe de usuario. *Ver* Informe personalizado
Informe del recurso. *Ver* Informe personalizado
Informe personalizado
acción de examinación de niveles inferiores, conexión 465
acción de examinación de niveles inferiores, parámetros 465
acción de examinar de niveles inferiores, acerca de 465
acción de examinar de niveles inferiores, especificar 465
acerca de 452
adición de expresiones de filtro en una consulta 535
campos de origen
adición a consulta de recursos 532
edición 544
campos de origen de consulta SQL 533

componentes 450
consulta 457
Ver también Consulta de informe
consulta de recurso 457
Consulta SQL 459
conversión de una consulta de recurso en una consulta SQL 457
creación 452, 455
editar 452
escribir una consulta SQL 533
examen de niveles inferiores de resultados 465
generación de una consulta de recursos 529
modificación 456
parámetro de consulta
acerca de 534
parámetro de informes
adición 460
adición de tipo avanzado 460
configuración 546
creación 460
modificación 460
parámetro de informes, definición 460
propiedades, especificación 468
vista de cuadrícula, acerca de 464
Ver también Vista de cuadrícula, informe
vista de gráfico, acerca de 462
Ver también Vista de gráfico, informe
visualización de consulta resuelta 537
visualización de resultados de consulta 538
Informes
administración habilitada para la nube 338
Informes de jerarquía
cómo actualizar datos de resumen 170
Instalación manual de Symantec Management Agent
selección de equipos 246
Instalación por primera vez
administración de parches 187
instantánea
creación a partir de resultados del informe 448
Instantánea de los datos del informe
depurar 80
IT Management Suite 7.5
novedades 25
nuevas funciones 25

J

Jerarquía
acerca de 153
configurar 156
creación de relaciones jerárquicas 157
crear relaciones jerárquicas 161
ejecutar políticas de automatización 168
ejecutar tareas 413
eliminación de un Notification Server 157
habilitación de la replicación 157
indicador de estado de la alerta 157
información de estado de tarea 413
informes 169
modificar relaciones jerárquicas 161
políticas de automatización 168
proceso de configuración 156
réplica manual de datos seleccionados 168
replicación. *Ver* Réplica de la jerarquía
requisitos 155
Jerarquía de Notification Server. *Ver* Jerarquía

L

Licencia
evaluación 30
soluciones 30
Limpiar
datos de la versión de la tarea 429
Limpieza
datos de tarea 429

M

Marco de Administración de software
acerca de 28
Mensaje
origen de datos para política de automatización 401
Mensajes de estado
cómo ver en el visor de registros 73
registro 72
Menú contextual
usar con los miembros del filtro 364
menú contextual
adición de la acción personalizada 55
adición de la línea de comandos 55
adición de URL 55
parámetros de sustitución de configuración 55
menú de la consola
adición de elementos de menú 53
adición de submenús 53
importación de submenú desde archivo XML 53
personalizar 53

N

Network Discovery 208–209, 212–213
acerca de 190
asistente 209
cantidad máxima de subprocesos 210
configuración 210
informes 219
métodos 216
proceso 209
resultados 219
seleccionar el intervalo de red 217
Tarea 213
Notas de la versión 31
Notificaciones por correo electrónico
configuración 72
Notification Server
acerca de 66
Base de datos de la administración de configuración 76
calendario interno de programaciones 124
cómo ver el archivo de registro 73
cómo ver mensajes de estado 73
configuración de dirección de correo electrónico 72
configuración de procesamiento 69
configuración del servidor proxy 74
configurar con el configurador de NS 75
configurar para la administración habilitada para la nube 302
configurar para usar HTTPS 287, 291
creación de relaciones jerárquicas 157, 161
descripción general 28
descripción general de la configuración 67
filtro. *Ver* filtro
funciones 66
identidad de la aplicación 69
introducción a las opciones de configuración 68
jerarquía 153
políticas. *Ver* Política
procedimiento de configuración 68
procesamiento de NSE 69
Ver también Procesamiento de NSE
programaciones 119
Ver también Programación
programaciones compartidas 122
registro de mensajes de estado 72
replicación 172
servicios de sitio 127, 138
Ver también Servicio de sitio
servidor de paquetes 138
Ver también Package Service
servidor de sitio. *Ver* servidor de sitio
sitio. *Ver* servicios
subred. *Ver* subred
tipos de configuración 67
uso de la programación 117

O

Operadores de búsqueda
acerca de 45
Optimización
configuración de agente y tareas 184
Optimizar la configuración del agente 181
Origen de datos
creación de una definición 479
especificación para política de automatización 401
uso de un informe para una política de automatización 401
uso de un mensaje para una política de automatización 401
uso de una consulta de recursos para una política de automatización 401
uso de una consulta SQL para una política de automatización 401

P

Package Server para Linux 141
acerca de 141
acerca de configurar con el servidor web Apache 145
acerca de configurar HTTPS y HTTP 146
acerca de integrar el servidor web Apache 142
detectar el servidor web Apache 143
ejemplos de configuración 147
plataformas admitidas 141
Package Service
configurar como Sin restricciones 139
establecer configuración 139
Página del portal
acerca de 59
Mi portal 59
página del portal
creación 59
modificación 59
Página inicial de Administración de Notification Server 51

Página Edición de informes personalizada
ficha Vistas 539, 542
Página Mi portal
acerca de 50
Paquete
Symantec Management Agent 273
Paquete de Symantec Management Agent
actualizar puntos de distribución 273
configuración 273
Paquete, software
actualizar puntos de distribución 370–371
adición de un programa 373
administrar programas 373
Configuración 370
habilitación del acceso desde una ruta UNC 372
quitar un programa 373
Parámetros
entrada 426
Parámetros de la entrada
recepción 426
pcAnywhere Solution
componentes de 29
funciones de 29
Perfil de conexión
acerca de 215
crear 215
Período de bloqueo
visualización en el calendario interno de programaciones 124
Permisos
acerca de 491
administración de credenciales 509
administración de recursos 505
asignación a un rol de seguridad 103
carpetas 507
categorías de permiso 491
cómo ver 113
filtros 508
informes 507
perfiles de conexión 508
políticas 507
sistema 506
Task Server 506
personalización
menú de la consola 53
Pertenencia al dominio
detección de recursos 190
Ping 216
Política
acerca de 376
actualización de Symantec Management Agent 268
actualización del agente 389
Administración 378
aplicar 378
basadas en el usuario 377
configuración global de agente 277
cuándo usarla con tareas y trabajos 412
desinstalación de Symantec Management Agent 268
desinstalación del agente 389
instalación del agente 389
política de automatización basada en un mensaje 398
política de automatización programada 396
política de ventana de mantenimiento 280
políticas de automatización 391
Ver también Política de automatización
políticas de automatización de jerarquía 168
programación 387, 424
tipos 376
Vista Políticas 378
política
destino, especificar 379
visualización en el calendario interno de programaciones 124
Política de automatización
acción 392
acerca de 391
activación y desactivación 393
administración 393
cómo crear programado 396
cómo modificar programado 396
componentes 392
creación de mensaje basado en 398
creación de tarea 405
desencadenador 392
ejecución de acciones en 393
eliminación 393
especificación de origen de datos 401
establecimiento de la seguridad en 393
establecimiento de regla de evaluación 396, 398
jerarquía 168
modificación de mensaje basado en 398
modificación de tarea 405
origen de datos 392
prueba 393

regla de evaluación 392
política de automatización
especificar la acción 403
visualización en el calendario interno de programaciones 124
Política de Configuración de administración habilitada para la nube
configurar 320
deshabilitar 320
habilitar 320
Política de registro de agente
crear 243
Portal de trabajos y tareas
acceder a 432
Privilegio, seguridad
acción con botón derecho 500
acción de administración de software 503
acción específica de la solución 503
administración 492
asignación a un rol de seguridad 93
categorías 489
credencial 496
directorio del flujo de trabajo 497
elemento de estado de activo 505
jerarquía 502
muestras del conector 502
perfil de conexión 492
réplica de la jerarquía personalizada 165
sistema 494
Symantec Management Console 497
Procesamiento de NSE
activación manual 69
configuración 69
Procesamiento del servidor
configuración 69
Programación
activación 119
actualizaciones de pertenencia a recursos 367
aplicación a la política 387
compartida 119
componentes 119
configuración 123
incluir varias programaciones 123
instalación programada de Symantec Management Agent 249
intervalo de fechas activas 123
modificantes 119
período activo 119
personalizada 119
política de agente 119
política del servidor 118
tarea del agente 118
tarea del servidor 118
usos en Notification Server 117
Ventana de mantenimiento 119
visualización del calendario de programaciones de Notification Server 124
zona horaria 119
Programación compartida
acerca de 122
creación 122
eliminación 122
habilitar 122
modificación 122
visualización de usuarios de la programación 122
visualización en el calendario interno de programaciones 124
Programación de actualización completa
configuración 367
Programación de actualización de políticas
configuración 367
Programación de actualización delta
configuración 367
Propiedades
entrada 426
Propiedades de la entrada
recepción 426
Puntos de distribución de paquetes
actualización 371
cómo especificar las credenciales 75

R

Realizar ajuste automático de la configuración del agente 181
Realizar instalación distribuida del agente 181
Recurso
adición a un grupo organizativo 436
Recursos
acerca de 470
actualizaciones de la pertenencia al filtro 363
cómo ver información de clase de datos 471
cómo ver la información de tipo de asociación de recursos 471
cómo ver la información de tipo de recurso 471
ejecución de acciones en miembros del filtro 364
excluir del filtro 361
incluir en filtro 361
seguridad. *Ver* Seguridad de recursos

recursos
actualizaciones programadas del filtro 367
selección mediante un filtro 353
Recursos de Notification Server. *Ver* Recursos
Registro detallado
depuración 487
Regla de CMDB
ejecutar como tarea 485
Regla de exportación
crear 480
Regla de importación
crear 480
Regla de transferencia de datos
comprobar 483
ejecución 482
Reglas de CMDB
acerca de 484
Reglas de replicación
replicación 175
reglas de replicación
réplica de la jerarquía 163
Réplica de la jerarquía
configuración 163
elementos 163
objetos de seguridad 163
recursos 163
reglas de replicación 163
réplica diferencial 163
réplica manual de datos seleccionados 168
replicación completa 163
replicación personalizada 165
Sobrescritura de la programación de réplicas diferenciales 167
Replicación
acerca de 172
completa 172
configuración 175
creación de reglas de replicación 175
diferencial 172
ejecución de reglas de replicación 175
elementos 175
eliminación de reglas de replicación 175
eventos 175
habilitación de reglas de replicación 175
jerarquía. *Ver* Réplica de la jerarquía
recursos 175
reglas de replicación 175
requisitos 174
seguridad 175
Replicación de Notification Server. *Ver* Replicación
Requisitos previos
Instalación de Symantec Management Agent 242
instalación de Symantec Management Agent para UNIX, Linux y Mac 258
Rol de seguridad
adición de miembros 101
asignación al grupo organizativo 346
asignación como miembro de otros roles 103
asignación de permisos 103
asignación de privilegios 93
categorías de privilegio 489
configuración de permisos de herencia en carpetas 104
configuración de permisos personalizados en el grupo organizativo 346
predefinido 107
predeterminado 107
privilegios de acción de administración de software 503
privilegios de acciones del menú contextual 500
privilegios de administración 492
privilegios de credenciales 496
privilegios de directorio de flujo de trabajo 497
privilegios de elementos de estado de activo 505
privilegios de jerarquía 502
privilegios de muestras del conector 502
privilegios de Symantec Management Console 497
privilegios de tareas de elemento 500
privilegios del perfil de conexión 492
privilegios del sistema 494
propiedad de una carpeta o elemento 115
réplica de la jerarquía personalizada 165
seguridad de recursos 340
Roles de seguridad
acerca de 89
configuración 89
creación 89

S

Secuenciación
tareas 416
Seguridad
acerca de 84
administrar 109
cómo desbloquear las credenciales 113
configuración 85

configuración de la complejidad de la contraseña 110
configuración del bloqueo de la contraseña 110
recursos. *Ver* Seguridad de recursos
roles predefinidos 107
roles predeterminados 107
Seguridad de recursos
acerca de 340
configuración de la seguridad en un grupo organizativo 346
configuración de permisos de seguridad personalizados en el grupo organizativo 346
grupos organizativos 344
proceso de configuración 340
vistas organizativas 343
señal
Task Server 410
Servicio de sitio
establecer configuración 138
Servicio de tareas
establecer configuración 139
servidor de sitio
adición de servicios de sitio 131
administración 131
asignación manual al sitio 133
creación 131
estado 131
modificación 131
quitar del sitio 131
quitar servicios de sitio 131
Servidor proxy
configuración 74
Servidores de paquetes
configuraciones 517
configurar para la administración habilitada para la nube 302
publicar las bases de código de HTTPS 302
Servidores de sitio
asignar a un sitio 304
configurar para los agentes habilitados para la nube 304
instalar el certificado 296
Sincronización de datos
Ejecución manual de réplicas de la jerarquía 167
jerarquía de Notification Server 153
réplica de la jerarquía 163
replicación entre equipos con Notification Server 172
requisitos de la jerarquía 155
requisitos de réplica 174
Sitio
administración 129
configurar para los agentes habilitados para la nube 304
creación 129
mantenimiento del sitio 128
modificación 129
Package Server sin restricciones 139
servicios de sitio 127
servidor de sitio 128
sitio
asignación de subred 135
asignación manual de agentes 134
asignación manual del servidor de sitio 133
eliminación 129
Eliminación de una subred 129
eliminación del servidor de sitio 129
Sitio web de IIS
configuración 310
Sitio web de IIS para el agente de CEM
configuración 311
Software
buscar 42, 45
Solicitud de registro del agente
bloquear 251
permitir 251
Solución de problemas 511
Solución de problemas de la línea de comandos 511
Soluciones
instalación 30
licencia 30
subred
administración 135
asignando al sitio 135
eliminación 135
resincronización 135
Symantec Management Agent
acerca de 236
actualización 266
asignación manual al sitio 134
configuración de destino 278
configuración de políticas de agente 276
configuración de una política de ventana de mantenimiento 280
configuración global 277
configuración local 278
desinstalación manual 274
desinstalar 267

importación de equipos desde el archivo .CSV 246
informe del estado de instalación 250
instalación en equipo desconectado, proceso 323
instalación programada 249
instalación remota manual 247
instalar automáticamente en equipos Windows 246
instalar en equipos Windows seleccionados 246
intervalos de actualización de datos 510
métodos de actualización 266
métodos de desinstalación 267
métodos de instalación 238
Paquete 273
Ver también Paquete de Symantec Management Agent
parámetros del paquete de instalación 522
política de actualización 268, 389
política de desinstalación 268, 389
proceso de instalación manual 240, 255
realizar instalación distribuida 181
redirección para usar HTTPS 287, 295
requisitos de instalación 242
requisitos previos 242
selección de equipos para la instalación 246
solucionar problemas 511
solucionar problemas para la administración habilitada para la nube 327
ventana de mantenimiento 280
Symantec Management Agent para UNIX, Linux y Mac
acerca de 236
archivo de plantilla .csv 256
creación de un archivo .csv para almacenar información detallada de los equipos 256
especificar la configuración de instalación 259
informe del estado de instalación 250
instalación automática en los equipos 260
instalación en equipos seleccionados 260
instalación remota manual 264
métodos de instalación 238
paquete 273
Ver también Paquete de Symantec Management Agent
política de actualización 268
política de desinstalación 268
proceso de instalación manual 255
requisitos de instalación 258
Requisitos previos 258
tareas de instalación simultáneas, configurar 260
Symantec Management Agent para Windows
importación de equipos desde un archivo CSV 246
selección de equipos para la instalación 246
Symantec Management Console
acceso 48
acceso local 48
acceso remoto 48
acerca de 34
ayuda 50
componentes personalizables 52
documentación 50
Elemento web. *Ver* Elemento web
guardar elementos como archivos XML 63
guardar submenú como archivo XML 53
importación del menú de un archivo XML 53
menú. *Ver* menú de la consola
Página del portal. *Ver* Página del portal
página principal 51
personalización 34
personalizar 52
visualización. *Ver* vista de consola
Symantec Management Platform
acerca de 24, 28
componentes 28
introducción 24
seguridad 84–85, 109
Symantec Management Platform 7.5
novedades 25
nuevas funciones 25

T

Tarea
acción de política de automatización 403
creación 418
creación para política de automatización 405
cuándo hacer uso 412
dependencia en filtro 365
destino, especificar 379
ejecución 421
especificar parámetros de entrada 403
modificación para política de automatización 405
programación 424
secuenciación 416
seleccionar para la política de automatización 404
visualización en el calendario interno de programaciones 124

tarea de Detección de red
configuración de protocolo 214
creación 213
modificación 213
perfil de conexión 214
ubicación 213
Tarea de detección de redes
cómo delegar 226
cómo habilitar Supervisores de Symantec para que creen 226
tarea de Network Discovery
creación 212
ubicación 212
Tareas y trabajos
ejecución 420
Task Server
aplicación de escala 417
configuración 430
implementación 417
señal 410
Trabajo
creación 418
cuándo hacer uso 412
ejecución 421
programación 424
secuenciación 416
Transferencia de datos
configuración 480
configurar 477
resúmenes 483

U

Usuarios
políticas basadas en el usuario 377

V

Ventana Catálogo de software
acerca de 43
Ventana de mantenimiento
configuración de política 280
visualización en el calendario interno de programaciones 124
Visor de registros
abrir 73
vista de consola
acerca de 36
adición de componentes 58
adición de vínculos de elementos 58
adición de vínculos web 58
creación 57
modificación 57
suplantación de árbol 36
Vista de cuadrícula, informe
acerca de 464
condiciones de formato 542
creación 464
formato avanzado 542
modificación 464
plantilla de formato 542
Vista de equipos
acerca de 36
Vista de gráfico, informe
acerca de 462
configuración del eje X 539
configuración del eje Y 539
creación 462
leyenda del gráfico 539
modificación 462
título del gráfico 539
zoom 3D 539
Vista organizativa
acerca de 343
crear 343
filtrar grupos que se muestran 343
modificar 343
uso en la seguridad de recursos 340
vista predeterminada 343
Vista Políticas
acerca de 44
Vista Software
acerca de 41
Vista Trabajos y tareas
acerca de 44
Vistas mejoradas
acerca de 36, 41
aplicar la política 378
configuración 47
ejecución de tareas y trabajos 420
vista de equipos 36
vista del software 41
Vistas organizativas
ver los dispositivos detectados 219
Vistas y grupos organizativos
crear 343
rellenar 343